What Is Known from a Network?

Digital Contact Tracing, Privacy, and Pandemics in the Digital Age

Kelsie Nabben, Marta Poblet, and Jan Carlo Barca

WORKING PAPER

COVID-19 RESPONSE

MERCATUS CENTER
George Mason University

Suggested Citation

Kelsie Nabben, Marta Poblet, and Jan Carlo Barca. "What Is Known from a Network? Digital Contact Tracing, Privacy, and Pandemics in the Digital Age." Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, October 2020.

Author Affiliation and Contact Information

Kelsie Nabben
Researcher
Blockchain Innovation Hub / Digital Ethnography Research Centre, RMIT University
kelsie.nabben@rmit.edu.au

Marta Poblet
Associate Professor
Graduate School of Business and Law, RMIT University

Jan Carlo Barca
Senior Lecturer
Information Technology, Deakin University

Disclaimer

Mercatus Center at George Mason University
3434 Washington Blvd., 4th Floor
Arlington, VA 22201
www.mercatus.org
703-993-4930

This paper can be accessed at https://www.mercatus.org/publications/covid-19-crisis-response/what-known-network

What Is Known from a Network?

Digital Contact Tracing, Privacy, and Pandemics in the Digital Age

Kelsie Nabben, Marta Poblet, and Jan Carlo Barca

Abstract: COVID-19 is an unprecedented crisis that has sparked unprecedented responses from governments around the world. These responses pose a threat to democratic stability and civil liberties. Digital contact tracing is just one example of a technology-based crisis response measure that has been rapidly deployed but could have far-reaching negative consequences for society. This paper explores the risks and consequences of collecting, collating, and storing digital data on people's networks of contacts as a crisis response measure. We aim to inform a discussion on the tradeoffs between the value of creating the data for public health outcomes and the risks to public trust in government and democratic stability. We ask, "What are the privacy risks of digital contact tracing, and what consequences does this have for national security and democratic stability?" We analyze the considerations that governments are taking in designing and deploying digital responses to the crisis in the case of digital contact tracing, and we explore what information can be derived from the data on populations and how this information could be misused in ways that harm democratic principles. We argue that government collection of digital contact tracing data poses a serious threat to civil liberties owing to the potential for the data to become a geopolitical target for hacking and interference in democratic stability through information warfare. We then propose a number of technical considerations and policy settings that are transparent, temporary, and proportionate to limit data vulnerabilities and provide a framework to better safeguard civil liberties and democracy in the digital age.

JEL codes: O33, O38

Keywords: digital, contact tracing, privacy, democracy, decentralization

The digital and public health policies deployed to contain COVID-19 have produced an unprecedented acceleration toward draconian digital surveillance measures around the world. They include the use of digital contact tracing. Smartphone-based contact tracing apps are widely viewed as an important tool for curbing the spread of the virus, but there is little evidence of their effectiveness. Human rights groups, meanwhile, warn that contact tracing apps pose huge privacy risks. In the rush to embrace this "solution" to the pandemic, policymakers have failed to fully consider the privacy risks and implications of digital contact tracing.

In this paper, we explore the privacy risks of digital contact tracing, as well as the consequences to national security and democratic stability of ill-considered digital responses to crise. To do this, we analyze the key considerations in the debate between civil society and government in the design and deployment of digital contact tracing apps and data storage processes, what is known about individuals and groups from network data collected by digital contact tracing apps, and the national security risks of information warfare and implications of collecting this type of data for democratic processes and stability.

We then propose digital infrastructure design and legal policy measures to support government to foster civil liberties and democratic principles to respond to both COVID-19 and future crises. By collaborating with the private sector and fostering local entrepreneurship, policymakers can embrace technology design approaches that are private by design and contextually appropriate, and thereby reduce the risks of creating and protecting sensitive stores of data.

1. The Problem: Unknown Consequences of Rapid Digital Responses to COVID-19

In response to COVID-19, governments across the world have adopted extraordinary measures to contain the spread of the coronavirus, including closing internal and external borders, locking down entire populations, and imposing curfews. Because this is the first pandemic of the digital age, technology-driven solutions have accompanied legislative responses to the crisis.

The use of government-issued digital tools has proliferated in the name of "disease surveillance"[1] and the "war on COVID."[2] This includes the use of surveillance cameras and facial recognition in Russia, mobile phone tracking in Taiwan, credit card data tracing in South Korea,

[1] Bill Gates, "How to Respond to COVID-19," *GatesNotes*, February 28, 2020.
[2] Giovanni Dell'Ariccia et al., "Economic Policies for the COVID-19 War," *IMF Blog*, April 1, 2020.

digital health passport ratings in China, and surveillance drones and ankle tracking bracelets in Australia. Population tracing in response to the virus first emerged in China,[3] but the trend quickly spread, along with the virus, to South Korea, Singapore, Taiwan, Europe, and Australia.

Mobile-phone-enabled contact tracing has emerged as a popular method of digital contact tracing. Multiple countries have adopted a technical policy that requires mass data collection on civilian populations, and thus enables tracking of entire populations. A new generation of government-sponsored digital contact tracing apps has repurposed the GPS or Bluetooth capabilities embedded in every "smart" mobile phone to track proximity to potentially infected members of the public. Meanwhile, observers around the world are urging caution: academics and industry experts in the United States, Australia, the United Kingdom, and Norway have signed joint statements urging governments to protect civil liberties as they implement digital contact tracing apps.[4]

The deployment of new technology during a crisis necessarily brings new challenges to the right to privacy, to public trust, and to societal stability.[5] The process of collecting data on people's location and contacts has required governments to design and deploy technical infrastructure that provides transparency and legal assurances to the domestic population, while

[3] Glenn Cohen, Lawrence O. Gostin, and Daniel J. Weitzner, "Digital Smartphone Tracking for COVID-19: Public Health and Civil Liberties in Tension," *JAMA*, May 27, 2020.
[4] "Joint Civil Society Statement: States Use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights," April 2, 2020, https://newamericadotorg.s3.amazonaws.com/documents/Joint-statement-COVID-19-and-surveillance.pdf; "Joint Statement," April 29, 2020, https://drive.google.com/file/d/1uB4LcQHMVP-oLzIIHA9SjKj1uMd3erGu/view; Joint Statement Norway, "Joint Statement on Contact Tracing for Norway," *Medium*, May 19, 2020; "Call for an Open Transparent Covid App: Statement from Academic and Industry Experts," accessed June 4, 2020, https://covidapp.opentransparent.org; "Call for an Open and Honest COVID Tracking App," accessed June 4, 2020, https://docs.google.com/document/d/1T-CVzfKDTZOK7DYUyHNR4RsoN4uuKcQux8UvYU9u6AE/edit.
[5] "Constitution of the United States," Constitution Annotated, accessed August 23, 2020, https://constitution.congress.gov/constitution; "Privacy and Human Rights: An International Survey of Privacy Laws and Practice," Overview section, Global Internet Liberty Campaign, accessed August 23, 2020, http://gilc.org/privacy/survey/intro.html.

protecting the data that is collected from becoming a target for foreign interference.[6] Government's methods of collecting and storing data obtained by digital contact tracing require further investigation regarding the implications for individual and national privacy and security.

The following section provides an in-depth analysis of digital contact tracing, exploring in more detail these themes of democracy, civil liberties, and privacy in the time of COVID-19.

2. Investigation of Design and Deployment of Digital Measures during COVID-19

In this paper, we focus on digital contact tracing as a case study because of its widespread adoption and the debate on privacy implications regarding a "centralized" versus a "decentralized" technical design. In the context of government-administered digital systems, "centralization" refers to computing architecture in terms of whether a system relies on a central server or "single point of failure" which, if it fails, can compromise the integrity of the entire system technically and politically in terms of who issues, administers, and accesses a system.[7] In contrast, "decentralization" refers to locally stored data, of which individuals retain sole ownership on their devices, and data are not aggregated and stored.

What Is Digital Contact Tracing?

Contact tracing is the process of interviewing victims of a viral disease to trace who they have been in contact with. Manual contact tracing is an established method for early warning, detection, and prevention of transmission in public health crises.[8] Contact tracing is not new, but the digitization of this process and collection of contact and mobility data on entire populations

[6] "Constitution," Constitution Annotated; "Privacy and Human Rights," Global Internet Liberty Campaign.
[7] Vitalik Buterin, "The Meaning of Decentralization," *Medium*, February 6, 2017.
[8] Ashley L. Greiner et al., "Addressing Contact Tracing Challenges—Critical to Halting Ebola Virus Disease Transmission," *International Journal of Infectious Diseases* 41 (December 1, 2015): 53–55; Glenn Webb et al., "A Model of the 2014 Ebola Epidemic in West Africa with Contact Tracing," *PLoS Currents* 7 (January 30, 2015).

during the COVID-19 crisis is unprecedented. Smartphone-based contact tracing apps have been developed with different technical and legal approaches in different parts of the world.

How Does Digital Contact Tracing Work?

Location tracking and social graph technologies have been available for some time, yet they have not before been openly deployed at a nation-state level. Singapore was one of the first countries to launch a Bluetooth-enabled smartphone-based tracing app in response to COVID-19.[9] The two aspects of the technical design of the system are what happens on a user's phone and what happens on the centralized data server. For Singapore's "TraceTogether" implementation, users set a PIN locally on the app, which is shared only with the Ministry of Health to release the contact tracing data if diagnosed. User data are stored locally on the user's device and deleted after 21 days or, if the user is diagnosed with COVID-19, are uploaded to a central database. The data are then analyzed and used by the Ministry of Health to contact people who have been in proximity with those diagnosed for faster warning and testing. Singaporeans are required by law to assist in the activity mapping of their movements and interactions by sharing data if contacted by the Ministry of Health once they have the app, including sharing data collected and stored by other popular apps in phones.[10]

With contact tracing apps and accompanying policies being implemented in different ways around the world, we outline some of the debates and tradeoffs in the design of these tools across different jurisdictions to surface some of the complexities in technical considerations

[9] TraceTogether (website), accessed April 9, 2020, https://www.tracetogether.gov.sg.
[10] "Can I Say No to Uploading My TraceTogether Data When Contacted by the Ministry of Health?," TraceTogether, updated September 9, 2020.

when rapidly deploying crisis response tools and considering civil liberties and possible consequences.

Mandatory or Voluntary?

Singapore's Ministry of Health took an opt-in, noncoercive policy approach for citizens toward downloading the app, but a mandatory approach toward data sharing once the app is downloaded. In Australia, there were some communication errors on whether the national contact tracing would be compulsory. Initial statements said it could be compulsory, in exchange for easing lockdown restrictions. Statements of coercion were later repealed, in line with the Biosecurity Emergency legislation to reinforce that the app would not be compulsory.[11] Other countries, such as China and Israel, opted to use existing mobile records to conduct contact tracing without consent.[12]

Centralized or Decentralized?

Centralized storage refers to contact tracing data being uploaded to a central data server, as opposed to being stored locally on a person's phone. Initially, Germany experimented with open data and data donation initiatives via wearable fitness trackers. Yet this approach was criticized on the basis of data privacy.[13] In terms of contact tracing apps, Germany initially backed a centralized specification that aimed to support international interoperability with the Pan-

[11] Jordan Hayne and Georgia Hitch, "Coronavirus App Will Not Be Forced Upon Australians, Scott Morrison Says," ABC News, April 18, 2020.
[12] Patrick Howell O'Neill, Tate Ryan-Mosley, and Bobbie Johnson, "A Flood of Coronavirus Apps Are Tracking Us. Now It's Time to Keep Track of Them," *MIT Technology Review*, May 7, 2020; Ruth Levush, "Israel Security Agency's Involvement in COVID-19 Tracing Scrutinized," *In Custodia Legis: Law Librarians of Congress*, May 7, 2020.
[13] Corona-Datenspende, Robert Koch-Institut (website), accessed April 9, 2020, https://corona-datenspende.de; "CCC Analysiert Corona-Datenspende Des RKI," Chaos Computer Club, April 20, 2020, https://www.ccc.de/de/updates/2020/abofalle-datenspende.

European Privacy-Preserving Proximity Tracing (PEPP-PT) standard that was purportedly General Data Protection Regulation (GDPR) compliant.[14] Following criticism regarding the legitimacy of this design from the scientific community related to centralized collection methods, the German government reversed the initial decision and opted to support a decentralized solution.[15] The Danish government also aimed to adopt a more privacy-preserving approach, based on the Decentralized Privacy-Preserving Proximity Tracing (DP3T) specification, along with Austria, Bulgaria, Canada, Estonia, and Switzerland (noting that varying degrees of stringency were taken on time limits and data destruction).[16] The European Commission and the European Data Protection Board also concluded that a decentralized model is more in line with EU data protection law.[17]

Open Source or Closed Source?

Sharing the software code of contact tracing apps allows software engineers, cryptographers, and other scientific and technology experts to verify if the app runs as described, alert for errors in the code, and suggest improvements. Open-source code is best practice in many software infrastructure communities, such as the Linux operating system.[18] In contrast, Australia released the app source code two weeks after releasing the app, but the server-side code has not been released. This means that there is no transparency or third-party verification on how data are aggregated, analyzed, or encrypted on the server side of the system, where it is collected and stored. Bluetooth-based apps collect proximity data on each person who comes within range of

[14] Douglas Busvine and Andreas Rinke, "Germany Flips to Apple-Google Approach on Smartphone Contact Tracing," *Reuters*, April 26, 2020; O'Neill, Ryan-Mosley, and Johnson, "A Flood of Coronavirus Apps."
[15] Corona-Warn-App Open Source Project (website), accessed June 4, 2020, https://www.coronawarn.app/en.
[16] "DP-3T/Documents," GitHub, accessed May 27, 2020, https://github.com/DP-3T/documents.
[17] Samuel Stolton, "Vestager Urges EU Member States Not to Backtrack on 5G," EURACTIV.com, May 6, 2020.
[18] Eric S. Raymond, *The Cathedral and the Bazaar* (Sebastopol, CA: O'Reilly Media, Inc., 2001).

the user, based on signal strength, to track proximity between phones with the app running. Little is known, however, about what information is being derived from the data once collected and aggregated in a database.[19]

Government Issued or Private?

Private-sector providers have an increasingly important role given the volume and sensitivity of data being collected. Apple and Google announced a partnership for a digital contact tracing specification to enable app developers to build contact tracing apps that function on both iPhone and Android devices.[20] Switzerland has been the first country to launch an app based on this contact tracing model.[21] Amazon is providing data server infrastructure for both Australia and UK contact tracing services, raising concerns that the data will be accessible offshore under the US CLOUD Act.[22] Deloitte is reportedly taking advantage of fragmentation in the healthcare system in the United Kingdom by offering consulting services to local UK health authorities after winning a national contact tracing services contract.[23] Digital contact tracing has also established a precedent for surveillance in private contexts, such as workplaces, where employees can be coerced to adopt tracing measures.[24] Instead of this invasive measure, governments could issue an open-source app design specification to facilitate local innovation and market competition, which would allow citizens to choose what data standards they are

[19] Kelsie Nabben and Chris Berg, "The COVIDSafe App Was Just One Contact Tracing Option. These Alternatives Guarantee More Privacy," *Conversation*, April 30, 2020.
[20] "Apple and Google Partner on COVID-19 Contact Tracing Technology," Apple, April 10, 2020.
[21] Chris Smith, "Switzerland Is the First to Use Apple-Google Coronavirus Contact Tracing Technology," *BGR*, May 27, 2020.
[22] Linton Besser and Dylan Welch, "Australia's Coronavirus Tracing App's Data Storage Contract Goes Offshore to Amazon", *ABC News*, April 24, 2020.
[23] Robert Booth, "Deloitte Selling Contact Tracing Services to Local UK Health Officials", *Guardian*, September 30, 2020.
[24] Karen Hao, "Machine Learning Could Check If You're Social Distancing Properly at Work," *MIT Technology Review*, April 17, 2020; Estimote (website), accessed June 5, 2020, https://estimote.com.

comfortable with, as long as the data can be voluntarily uploaded if and when contact tracing becomes necessary.

Even if application developers adhere to the criteria to endeavor to build apps that are voluntary, decentralized, and open source, digital contact tracing apps have not been proved to be effective.

Effective or Ineffective?

Emerging evidence indicates that digital contact tracing is an ineffective measure for addressing public health outcomes. Independent reviews have found that there is a lack of evidence to support the immediate deployment of many of the proposed technical solutions.[25] For example, Iceland demonstrates one of the most successful responses to contain COVID-19, whereby the Department of Civil Protection and Emergency Management Team deployed a contact tracing app that is voluntary, transparent, and temporary. It had one of the highest adoption rates as a percentage of the population in the world, at 38.5 percent.[26] However, Iceland also largely attributes its success to having one of the most aggressive testing regimes in the world. Researchers are emphasizing that contact tracing apps cannot replace parallel public health measures, such as physical distancing and hygiene.[27]

There has been enormous pressure in Australia from the government to download the COVIDSafe digital contact tracing app. Federal Health Minister Greg Hunt was even accused of

[25] "COVID-19 Rapid Evidence Review: Exit through the App Store?," Ada Lovelace Institute, April 20, 2020.
[26] "Annex IV: Inventory Mobile Solutions against COVID-19," accessed May 29, 2020, https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_annex_en.pdf; "Covid Tracing Tracker—Read Only," accessed May 29, 2020, https://docs.google.com/spreadsheets/d/1ATalASO8KtZMx__zJREoOvFh0nmB-sAqJ1-CjVRSCOw/edit?usp=embed_facebook.
[27] Luca Ferretti et al., "Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing," *Science* 368, no. 6491 (May 8, 2020); Bobbie Johnson, "Nearly 40% of Icelanders Are Using a Covid App—and It Hasn't Helped Much," *MIT Technology Review*, May 11, 2020.

coercion for a Tweet insinuating that lockdown restrictions might be eased in exchange for civilian compliance with adopting the app.[28] Despite the pressure, the government reported that "we haven't found a number of additional contacts with the COVIDSafe app."[29] The app has been politicized at the state and federal level to be coined a "$2 million failure."[30]

Despite this evidence, multinational bodies such as the World Health Organization have proposed that the contact tracing approach be amplified, to form a global contact tracing database to track civilians across borders, alongside issuance of digital "health immunity passports."[31] The societal risks of such a resource are immense, including scope creep, lack of accountability, discrimination, coercion, hacking, and oppression.

In the next section, we highlight the importance of digital privacy as a civil liberty, before offering a more comprehensive understanding of what information can be ascertained from collating contact tracing data on a national level and how this may be used against populations.

3. What Can Be Known, and What Are the Risks?

Digital Privacy and Why It Matters

Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights, and many other international and regional treaties. Nearly every country in the world recognizes a right of privacy explicitly in its constitution or adjacent legal instruments. While "privacy" relates to freedom from outside

[28] Greg Hunt, "Want to Go to the Footy? Download the App," Twitter, May 1, 2020, https://twitter.com/greghuntmp/status/1256403073674739712.
[29] Maddy King, "Has the COVIDSafe App Been Used in the Recent Outbreaks?," *triple j Hack*, July 14, 2020.
[30] Jonathan Kearsley, "Fears COVIDSafe App Not Working as Intended," 9 News, June 25, 2020; Jonathan Kearsley, "COVIDSafe App a '$2 Million Failure,' Bowen Says," *Sydney Morning Herald*, July 13, 2020.
[31] Eliza Strickland, "An Official WHO Coronavirus App Will Be a 'Waze for COVID-19,'" *IEEE Spectrum*, March 20, 2020; *Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak*, European Data Protection Board, April 21, 2020.

interference, there is not one definition. It can be addressed as information privacy, involving the establishment of rules that govern the collection and handling of personal data; bodily privacy; privacy of communications; and territorial privacy.[32]

Data protection can be enforced both legally *and* technically. European legal instruments have been influential in shaping data privacy protection legislation around the world.[33] These rules are predicated on the right of people to access and amend their data (since they are the legitimate "owners"), as well as on the fair and lawful collection of data, the use of data for the original specified purpose and not excessive to the purpose, and the use of data that are accurate and that are destroyed after the stated purpose is completed.

Technical design, in terms of what capabilities are developed, deployed, and managed, is also a fundamental consideration in digital privacy. In the absence of adequate oversight, accountability, and enforcement, legal measures are not necessarily designed to protect civil society from privacy abuses. The response to COVID-19 demonstrates how some governments have deliberately exploited the crisis as an opportunity to pass decrees that erode privacy, undermine data protection rules, discriminate against marginalized groups, and constrain other civil liberties.[34] This is why privacy must also be considered in the technical design.

The risks of creating contact tracing data are multifaceted, both at an individual level and in terms of a large-scale network. The problem with the "I've got nothing to hide" argument is

---

[32] "Privacy and Human Rights," Global Internet Liberty Campaign.

[33] "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data," Council of Europe, accessed August 24, 2020, https://rm.coe.int/1680078b37; "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Organisation for Economic Co-operation and Development, accessed August 24, 2020, https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[34] K. D. Ewing, "Covid-19: Government by Decree," *King's Law Journal* 31, no. 1 (May 13, 2020): 1–24; Graham Greenleaf and Katharine Kemp, "Australia's 'COVIDSafe App': An Experiment in Surveillance, Trust and Law," *University of New South Wales Law Research Series 999*, April 30, 2020; Cheuk Hang Au and Kevin K. W. Ho, "Deliberation in Mobile Messaging Application: A Case in Hong Kong," *Communications of the Association for Information Systems* 45 (2019).

that privacy is structural, meaning that revealing one person's network of contacts reveals information about others in the network and about the network as a whole.[35] Furthermore, data can be aggregated (combining pieces of information to uncover more information), owners can be excluded from accessing or deleting data (known as "exclusion"), and data can be used for purposes beyond their original intent (known as "secondary use").[36]

At an individual level, de-anonymizing data from human networks has been possible for years.[37] Contact tracing data can also be de-anonymized to re-identify individuals. A group of researchers in Denmark using Bluetooth-based proximity data, alongside other basic indicators like online social media contacts, found that individuals can be easily identified.[38] When influential individuals or certain social groups in a society are de-anonymized, information warfare techniques, such as online misinformation and disinformation, can be used for planned attacks to polarize whole societies. According to the International Red Cross Movement, unsuitable design or usage of contact tracing apps could lead to stigmatization, increased vulnerability and fragility, discrimination, persecution, and attacks on the physical and psychological integrity of certain populations.[39] The consequences of the exposure of private and

[35] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Redwood City, CA: Stanford University Press, 2009).
[36] Daniel J. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Review* 44 (2007): 745.
[37] Arvind Narayanan and Vitaly Shmatikov, "Robust De-Anonymization of Large Sparse Datasets," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*, Oakland, CA, 2008, 111–25; Sébastien Gambs, Marc-Olivier Killijian, and Miguel Núñez del Prado Cortez, "De-Anonymization Attack on Geolocated Data," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Melbourne, VIC, 2013, 789–97; Wei Peng et al., "A Two-Stage Deanonymization Attack against Anonymized Social Networks," *IEEE Transactions on Computers* 63, no. 2 (February 2014): 290–303.
[38] Vedran Sekara, Arkadiusz Stopczynski, and Sune Lehmann, "Fundamental Structures of Dynamic Social Networks," *Proceedings of the National Academy of Sciences* 113, no. 36 (September 6, 2016): 9977–82.
[39] Balthasar Staehelin and Cecile Aptel, "COVID-19 and Contact Tracing: A Call for Digital Diligence," *International Federation of Red Cross and Red Crescent Societies*, May 15, 2020.

personal data would be extremely damaging in a divided environment that is affected by armed conflict, violence, disaster, communal tensions, or economic inequalities.[40]

What Network Data Reveal

Large datasets reveal incredible amounts of information. Mobile phone apps collect background information when downloaded, such as phone model, device name, other apps running, and Wi-Fi routers accessed. Wi-Fi signal information can be easily converted into precise geographical position.[41] Furthermore, if router information is known at a single point in time, it can produce highly detailed information about the movement patterns of people.[42]

In Norway, GPS location data from the government-issued contact tracing app were continuously uploaded in real time, allowing for de-anonymization and live tracking of individuals, including armed forces personnel.[43] The Norwegian Minister of Digitalization has been called upon to respond to the malpractice at the ministerial level and internationally via the European Commission, and human rights advocate Amnesty International has condemned the reckless approach to digital data collection.[44] The app has since been withdrawn, and all data collected has reportedly been deleted.[45] This is not the only example of the risks of digital contact tracing to privacy and security.

---

[40] Staehelin and Aptel, "COVID-19 and Contact Tracing."
[41] Thor S. Prentow et al., "Spatio-Temporal Facility Utilization Analysis from Exhaustive WiFi Monitoring," *Pervasive and Mobile Computing*, 16, part B (January 2015): 305–16.
[42] Sune Lehmann, "Tracking Human Mobility Using WiFi Signals," *Sune Lehmann*, May 26, 2015.
[43] Martin Gundersen and Trude Furuly, "Hofstad Helleland Om Mobilsporings-Avsløringen:—Dypt Urovekkende," NRK Norge, May 20, 2020.
[44] "Bahrain, Kuwait and Norway Contact Tracing Apps among Most Dangerous for Privacy," Amnesty International, June 16, 2020.
[45] Natasha Lomas, "Norway Pulls Its Coronavirus Contacts-Tracing App after Privacy Watchdog's Warning," *Techcrunch*, June 16, 2020.

Germany was going to adopt the relatively centralized digital contact tracing app specifications set out by PEPP-PT. PEPP-PT states in its formal documentation that insider attacks by administrators and state-level adversaries are "outside of scope" for security in the design of the system.[46] A privacy and security assessment by technologists, legal experts, engineers, and epidemiologists found that anyone with access to back-end server data could identify any specific, pseudonymous individual because the back-end user creates the ephemeral identifiers, and the back-end server can link any past or future identifier with the permanent identifier.[47] This information could be correlated with a small amount of additional data (such as camera footage or travel card data) to derive the identity of an individual or track someone long-term through a specific identifier. The data protection and security architecture of the PEPP-PT approach compromises the data minimization principle of GDPR by having access to more information than required. This poses a severe risk as administrators or hackers can learn the entire contact network of an individual, re-identify individuals, or persistently trace individuals. Civil society, including citizens and community groups, protested the approach, and Germany settled for a more data-privacy-preserving system.[48]

At mass scale, such as that of an entire population, the risk of creating pools of data on networks of people is amplified. This will be discussed further in the following section, to inform a discussion on the tradeoffs between the value of creating the data for public health outcomes, versus the risks to government, civil society, and democratic stability.

[46] "Pepp-Pt/Pepp-Pt-Documentation," GitHub, accessed May 27, 2020, https://github.com/pepp-pt/pepp-pt-documentation.
[47] "DP-3T/Documents," GitHub.
[48] "10 Requirements for the Evaluation of 'Contact Tracing' Apps," Chaos Computer Club, April 6, 2020.

Practical Dangers of Creating Digital Contact Tracing Databases

Several issues can arise when contact tracing data are harvested and stored without taking appropriate privacy measures. The data can be sold or handed over to third parties by members of the organization that undertakes the contact tracing exercise. The data can also be hacked by governments, groups, or individuals. In this setting, hostile social engineers, who attempt to regulate the future behavior and development of a society, can re-identify and de-anonymize groups of people by analyzing their whereabouts over time.

Once the contact tracing data has been de-anonymized, expert social engineers can mine the information via passive network imaging tools that reveal the underlying social structure, or topology, of the network.[49] All that is required to achieve this is information on the relative movement of the de-anonymized groups, which can be easily achieved by tracking actors in a network over time.[50] In a contact tracing scenario, this movement is represented by contacts or no contacts across individuals in the population.

The topology of a society, which commonly is represented by people in a network (nodes) and connections between people (edges), can then be exploited by social engineering professionals for information warfare purposes. Information warfare is the strategic use of online or communication technologies for advantage against an opponent. Psychological warfare is a component, which leverages misinformation, disinformation, and propaganda to influence, manipulate, confuse, and divide a constituency for a specific end. A number of state actors are

[49] Bruno Luis Mendivez Vasquez and Jan Carlo Barca, "Network Topology Inference in Swarm Robotics," *2018 IEEE International Conference on Robotics and Automation (ICRA)*, May 2018.
[50] Yathindu Hettiarachchige, Asad Khan, and Jan Carlo Barca, "Multi-Object Tracking of Swarms with Active Target Avoidance," *ICARCV 2018 : Proceedings of the 2018 15th International Conference on Control, Automation, Robotics and Vision*, November 2018.

capable of such attacks, with the aims of online propaganda, manipulation, election disruption, societal polarization, and unrest.[51]

Information warfare can be conducted via social network analysis tools that reveal influential nodes or groups of nodes. These nodes can be discovered by analyzing the number of links each node has to the broader society and the magnitude of its influence. Influential nodes are people that are highly trusted, whose ideas can then be influenced via online "memes," as a way to bypass skepticism and influence society. Memes are contagious forms of media, such as images, text, and music. Memes can be designed to propagate and manipulate, so they spread the idea. If weaponized, the aim of memes can be to autonomously recruit others to subscribe to an idea and form clusters of operational cells based on political ideology, religious beliefs, policy standpoint, or other potentially divisive issue.[52] When this is done in a strategic manner, certain messages are reinforced to create information echo chambers that are walled off from contrary information to reinforce extreme perspectives within a society.[53] Systematically, this generates more extreme viewpoints, which in turn can be exploited to polarize groups of differing opinions and fracture democratic or nondemocratic states.[54] The outcome can be a whiplash effect with conflict, violence, mass protests, or disruption of critical societal activities.

These operations can be made even more efficient by nefarious social engineering professionals if they take full advantage of existing technologies, such as social media

---

[51] Michael J. Mazarr et al., "The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment" (RAND Corporation, Santa Monica, CA, 2019).
[52] A. M. Nagy, *Cia: Manual for Psychological Operations in Guerrilla Warfare* (CreateSpace Independent Publishing Platform, 2011).
[53] Richard Brodie, *Virus of the Mind: The New Science of the Meme* (Carlsbad, CA: Hay House, 2011); J. C. Barca, C. Eales, and N. Choudhary, *Counter-Swarming—A Handbook* (Adelaide: Defence Science and Technology Group and Deakin University, 2020): 88.
[54] UK Government Secretary of State for Digital, Culture, Media & Sport and the Secretary of State for the Home Department, *Online Harms White Paper*, 2019, https://www.gov.uk/government/consultations/online-harms-white-paper.

advertising and internet of things devices (of which 100 billion are predicted to exist in homes, businesses, and public places by 2025). Such devices can be used to effectively harvest information from the population and to achieve data-driven behavior change, by injecting high-impact memes, collecting data to measure the response, and repeating.[55]

By creating and storing contact tracing data, the door to interference and exploitation in state stability is wide open. Digital and policy responses to crisis must be carefully measured against the risks of creating unnecessary data that may be exploited. And yet, digital contact tracing apps have not been designed to cope with these threats.

Challenges to Democratic Institutions

Crisis results in weakened democratic institutions and processes, making the risk of geopolitical exploitation even more pronounced. A number of scholars have pointed out the repercussions for the regular functioning of democratic institutions when states declare different levels of alert and state emergency, prorogue parliament sessions, or close both internal and external borders. For example, Schmitter contends that the pandemic response may turn some temporary dynamics into permanent trends: among others, enhanced centralization of decision-making, reduced face-to-face political participation, suspension of accountability mechanisms, or responsibility shifted to small groups of experts and their political allies.[56] In a similar vein, Flinders warns about the risk that the pandemic crisis may mutate into a broader democracy crisis by deepening the "trust

[55] Robin Taylor, David Baron, and Daniel Schmidt, "The World in 2025—Predictions for the Next Ten Years," *2015 10th International Microsystems, Packaging, Assembly and Circuits Technology Conference (IMPACT)*, October 2015.
[56] Philippe Schmitter, "Food for Thought about the Impact of the COVID-19 Virus upon the Institutions and Practices of 'Real-Existing' Democracy," *COVID-DEM*, April 17, 2020, 6.

gap" between politicians and citizenship, augmenting the blame games, and, more broadly, incrementing the "negativity bias" across the population.[57]

Challenges to Democratic Processes

Some scholarly literature also focuses on the potential impact of the pandemic on electoral processes. For example, Krimmer, Duenas-Cid, and Krivonosova examine the relationship between democracy and the current pandemic from an electoral angle and analyze the challenges of both postponing planned elections and holding them with adapted methods, such as postal or online voting.[58] Similarly, Landman and Di Gennaro Splendore look at the potential disruptions of the electoral cycle and the larger impacts for democracy.[59] The authors identify different risks for every step of the electoral cycle and propose to adapt solutions, such as online campaigning and meetings, hybrid forms of voting, and virtual parliaments, which private businesses and organizations have already quickly deployed and adapted to during the pandemic.

This analysis highlights serious concerns of setting a precedent for mass data collection in crisis response legislation and practice, as well as such a precedent's ramifications for societal stability amid weakened democratic institutions and processes. Critical analysis of the technical and governance design of digital infrastructures through deeply considered, expert-guided, privacy-preserving approaches is essential to halt the normalization of mass data collection on civilian populations in crisis response.

---

[57] Matthew Flinders, "Democracy and the Politics of Coronavirus: Trust, Blame and Understanding," *Parliamentary Affairs*, June 23, 2020.
[58] Robert Krimmer, David Duenas-Cid, and Iuliia Krivonosova, "Debate: Safeguarding Democracy during Pandemics. Social Distancing, Postal, or Internet Voting—the Good, the Bad or the Ugly?," *Public Money & Management*, May 22, 2020.
[59] Todd Landman and Luca Di Gennaro Splendore, "Pandemic Democracy: Elections and COVID-19," *Journal of Risk Research*, May 1, 2020. See also John Keane, "Democracy and the Great Pestilence," Albert Hirschman Centre on Democracy, Graduate Institute of International and Development Studies, April 14, 2020.

4. Policy Options and Recommendations

Both technical and legal approaches are needed to improve digital-political responses during the COVID-19 crisis and beyond.

Technical Approaches

Privacy is crucial to the design and implementation of digital architectures. The previous analysis of digital contact tracing apps has set out the decision space for just some aspects of the design considerations for technical architectures. A framework to guide decision-making toward software code-based guarantees and accountability on how data are handled is privacy by design.[60] Privacy by design means that privacy is taken into consideration throughout the entire engineering process.[61] Practically, this could mean choosing a decentralized database architecture, such as blockchain or other peer-to-peer protocols; implementing technical privacy measures, such as encryption and differential privacy; and open-sourcing all code.[62] Furthermore, personal identifiers could be de-linked, by relying on non-smartphone-based hardware devices for contact tracing, such as smart cards or other hardware, crowdsourced data donations, or open-data initiatives.[63] Code could be made more robust and more accountable to civil society through third-party auditing. Although any approach is not without challenges, including commitment from leadership and the socio-technical security elements of how

[60] Heng Xu et al., "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* 12, no. 12 (2011).
[61] Ann Cavoukian, "The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices," Privacy by Design, January 2011, 2.
[62] New America and Open Technology Institute, Statement to the Senate Committee on Commerce, Science, and Transportation, on "Enlisting Big Data in the Fight against Coronavirus," submission by Sharon Bradford Franklin, policy director, April 9, 2020, https://newamericadotorg.s3.amazonaws.com/documents/New_Americas_Open_Technology_Institute_Statement_for_the_Record.pdf.
[63] Kelsie Nabben, "S4: Simple, Secure, Survivable Systems. Human-First Crisis Technology Design Principles," *Medium*, June 9, 2020.

technology is used by people in practice, privacy by design offers a conceptual approach that aims to protect users and organizations from creating, sharing, managing, and needing to protect excess data to build public trust.[64]

Legal Approaches

Technology attributes, such as privacy by design and transparency of data architecture, must be matched by coinciding legal and policy measures. Policy responses that align with the human rights principles of transparent, temporary, and proportionate laws are conducive to achieving public health outcomes, privacy, and stability. The European High Commissioner for Human Rights has condemned digital communications surveillance and data collection, including on a mass scale.[65] If data must be collected, legal guidelines could include clear and transparent policy measures on how data are collected, processed, stored, accessed, and deleted.[66] The amount of data collected could also be minimized.[67] Minimizing the practice of governments collecting mass personal data will reduce the liabilities that come with collecting sensitive contact network data in the first place, and is more conducive to maintaining the public trust and political stability necessary to endure the crisis.

A Broader Context: Norms of Digital-Political Responses to Disaster and Public Trust

While the legal and technical details are important considerations for how digital contact tracing could be done better for the well-being of civil society, these issues largely detract from the

[64] Sarah Spiekermann, "The Challenges of Privacy by Design," *Communications of the ACM* 55, no. 7 (July 2012): 38–40.
[65] "Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development," American Civil Liberties Union, 2016.
[66] "COVID-19 Rapid Evidence Review," Ada Lovelace Institute.
[67] Nuria Oliver et al., "Mobile Phone Data for Informing Public Health Actions across the COVID-19 Pandemic Life Cycle," *Science Advances* 6, no. 23 (June 5, 2020).

broader context, which positions digital contact tracing within the need to limit technology-based, government-issued digital-political responses in crisis. Governments' lack of digital preparedness and the ensuing debates detract from urgent policy priorities, such as that of public health infrastructure and economic recovery. The rushed deployment of digital tools and the focus of debate on such measures undermines public trust in the government's ability to competently respond to crisis. Next, we propose technical and legal measures as a framework to improve digital-political responses to crisis. Given the prominence and risks of digital responses and accompanying policies in crisis, some ways that governments could take a more holistic response to the digital age are as follows:

- Society relies on digital infrastructures, which are embedded in interconnected systems of people, technology, governance, and norms. Acknowledging the risk and tradeoffs of deploying digital tools allows administrators to better consider the cost-benefit analysis of creating dangerous precedents. With this lens, digital infrastructure can be designed with embedded privacy principles and contextual awareness, when it is required. For digital infrastructures to be successful, policymakers must recognize people as the primary focus for protection and consider the long-term implications of how and when digital tools are used in the interests of civil society.[68]
- Digital infrastructure requires interdisciplinary expertise to competently analyze the possible consequences of introducing a system. Administrators can establish interdisciplinary, expert advisory groups on digital societies for advice, accountability, and independent third-party analysis before digital solutions are released and once they

[68] Kelsie Nabben, "From Threat Models to Trust Models for Technology We Can Trust," *Medium*, June 10, 2020.

are deployed. This approach was taken in Canada, with the establishment of the Society, Technology and Ethics in a Pandemic Expert Advisory Group (STEP).[69]

- Local-first, bottom-up technology solutions diffuse the responsibility away from governments to centrally coordinate faultless digital responses to crisis. Policy settings to support innovation can encourage entrepreneurs to lead, engage, and partner with responses in their local context.[70] There has been an explosion of local responses to combat the pandemic. "Maker" groups have built hardware and software tools and open-sourced the design for others to do the same to create solutions, including testing, ventilators, face masks, protective gear, disinfection, data analysis, and sanitation.[71] Taiwan has engaged in full-scale civic engagement through the "digital democracy," "civic hacker" initiative to spread health and safety guidelines online, share public health advice, and counter misinformation.[72] Open-source, local-first initiatives allow people to consider their privacy needs and afford people agency over which digital tools to adopt. This allows for decentralization from single-point-of-failure mass data aggregations through diverse, local, creative, innovative responses that share responsibility and trust throughout the community so that people can take responsibility for civil liberties locally.

[69] "Expert Advisory Group on Society, Technology & Ethics in a Pandemic (STEP)," CIFAR, May 7, 2020.
[70] Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington, VA: Mercatus Center at George Mason University, 2016); Darcy W. E. Allen, *When Entrepreneurs Meet: The Collective Governance of New Ideas* (World Scientific Publishing Europe, forthcoming).
[71] "Open Source COVID-19 Wiki," accessed August 24, 2020, https://covid.riat.at/corona; "Open Hardware Projects to Fight COVID-19," accessed July 14, 2020, https://n-o-d-e.net/covid.html.
[72] Pamela Kennedy, "Audrey Tang on Taiwan's Digital Democracy, COVID-19, and Combating Disinformation," Stimson Center, March 18, 2020.

Conclusion

The implications of overt, population-wide contact network data collection for civil liberties are unpredictable, uncontainable, far-reaching, and permanent. Government collection of digital contact tracing data as a crisis response measure poses a serious threat to civil liberties because of the potential for the data to be exploited through hacking, foreign interference, and population manipulation. Such practices pose a threat to individual privacy, public trust, and democratic stability.