Hague Centre for Strategic Studies

The COVID-19 pandemic:: two waves of technological responses in the European Union

Author(s): Klaudia Klonowska and Pieter Bindt

Hague Centre for Strategic Studies (2020)

Stable URL: http://www.jstor.com/stable/resrep24004

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms

Hague Centre for Strategic Studies is collaborating with JSTOR to digitize, preserve and extend access to this content.

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

HCSS Snapshot

The COVID-19 pandemic: two waves of technological responses in the European Union

Klaudia Klonowska, Assistant Analyst
Reviewed by Pieter Bindt, Strategic Advisor

April 2020

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

Introduction

On January 30th, 2020, the World Health Organization declared a novel coronavirus, COVID-19, a matter of Public Health Emergency of International Concern.[1] Seeing the rapid growth of infections and deaths, governments worldwide were quick to implement a variety of measures. Among them, technological solutions in the form of anonymized phone location tracking and contact tracing apps.

The use of technology has accelerated a pre-existing debate in Europe regarding the privacy protection of users. In recent years, the European Union has established numerous limitations to the exploitation of personal data. This includes for example the limitation on an indiscriminate sharing of personal data with US companies.[2] In 2014, a major court case established a "right to be forgotten" protecting users from indefinite retention of their data on online search platforms.[3] This was followed in 2015 by the *Schrems* case, in which the Safe Harbor decision was revoked and the transfer of personal data of EU citizens to servers in the US was largely limited.[4] Most recently, the General Data Protection Regulation (GDPR) of 2016 sets a groundbreaking and high standard of data protection.[5] Therefore, the use of phone location data to track people's movements and the emergence of contact tracing apps have both sparked concerns.

This paper discusses the use of technology as a response to the COVID-19 pandemic among the European Union Member States considering years-long European effort to increase privacy protection. This paper identifies two waves of technological solutions: first, the use of anonymized location data shared by telecommunications companies (hereinafter: telecoms) to monitor crowd movements; second, the emergence of contact tracing apps to speed up the procedure of identifying infected individuals. Both waves of technological solutions are discussed in terms of privacy, transparency, and effectiveness.

1. The first wave: anonymized phone location tracking

In February of 2020, with the first death from COVID-19 in France and a steep increase of positive cases in Italy, the coronavirus pandemic became a matter of significant concern in Europe.[6] After a number of drastic lockdown measures and an unprecedented closure of borders within the Schengen zone, various European

[1] "WHO Director-General's Statement on IHR Emergency Committee on Novel Coronavirus (2019-NCoV)."

[2] Reidy, "After Edward Snowden's Revelations about the NSA, What Is the EU Doing."

[3] C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.

[4] C-362/14 Maximillian Schrems v Data Protection Commissioner. The introduction of the EU-US "Privacy Shield" framework in 2016 established data protection requirements when transferring personal data.

[5] "Regulation (EU) 2016/678 of the European Parliament and of the Council (General Data Protection Regulation)."

[6] Moné, Mosher, and Woodward, "A comprehensive timeline of the new coronavirus pandemic, from China's first COVID-19 case to the present."

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

governments began the search for technological solutions. By early March, governments reported initiatives of business-to-government sharing of anonymized phone location data[7] to track the spread of COVID-19.[8]

It has been reported that anonymized phone location data is in use by the governments of Belgium, Austria, Estonia, France, Germany, Latvia, Greece, Portugal, Italy, and Spain.[9] The companies involved include Orange S.A., Tele2, A1, Deutsche Telekom, Vodafone, LMT, and numerous other providers.[10] In addition, laws permitting the government to access telecom databases were passed in Bulgaria and are underway in Lithuania and Slovakia.[11] This shows that (at least) 13 countries across the European Union have access to anonymized phone location data for the purpose of tracking people's movement.

1.1 Privacy

At the heart of the first-wave solutions lies the question regarding privacy. Telecom providers ensure that shared location data is anonymized and aggregated.[12] In order to achieve anonymization, companies use the k-anonymity technique,[13] which means that location data is aggregated in groups not smaller than 30 users and presented in a statistical format.[14] This prevents identification of individual behavior patterns and avoids the possibility of re-identification.

Anonymization of telecom data makes its processing and sharing lawful under EU law (including GDPR) without the consent of users.[15] This highlights a continued commitment of the European Union to privacy-by-design solutions.

1.2 Transparency

Neither the governments nor telecoms are obliged by law to disclose information about the processing and sharing of anonymous data, as it is excluded from the scope of

---

[7] Phone data location is "often a combination of Internet Protocol numbers and GPS or assisted GPS (A-GPS) data when used by mobile phones". Klimburg et al., "Pandemic Mitigation in the Digital Age," 6.

[8] Individualized location tracking techniques are beyond the scope of this paper.

[9] Mascini, "EU Expert on European Response to Virus"; Moné, "10 Countries Are Now Tracking Phone Data as the Coronavirus Pandemic Heralds a Massive Increase in Surveillance"; Wright, "Statistics Estonia to Study People's Movements during Emergency Situation"; Stupp, "Europe Tracks Residents' Phones for Coronavirus Research"; "Mobile Network Research Suggests People Leave Cities to Weather the Crisis"; "Vodafone Group's Five-Point Plan to Help Counter the Impact of COVID-19"; Álvarez-Pallete, "Telefónica Announces Measures Related to COVID-19."

[10] See the sources listed above.

[11] Николов, "Полицията получи безконтролен достъп до телефони и интернет връзки"; Verseck, "Coronavirus: Rule of Law under Attack in Southeast Europe"; Jegelevičius, "Lithuania Puts COVID-19-Related Prosecution above Human Rights."

[12] See for example, "Vodafone Group's Five-Point Plan to Help Counter the Impact of COVID-19."

[13] For more information see https://en.wikipedia.org/wiki/K-anonymity.

[14] Mascini, "EU Expert on European Response to Virus."

[15] Although, the GDPR permits to share sensitive data "when it is necessary for reasons of public interest in the area of public health", such as a pandemic. Mascini; "Regulation (EU) 2016/678 of the European Parliament and of the Council (General Data Protection Regulation)"; Wiewiórowski, "EU Digital Solidarity: A Call for a Pan-European Approach against the Pandemic."

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

GDPR.[16] However, with the growth of surveillance capabilities, many are asking how shared data is retained, what other data it is combined with, with whom else it is shared, and what legal safeguards are in place. Answers to these questions are not easily obtained.

The Belgian Ministers of Health and Digital Agenda have ensured that the arrangement of data sharing is reviewed and continuously monitored by an ethics committee.[17] The German Data Protection Officer confirmed that shared data was legally compliant.[18] Amongst telecommunications companies, Vodafone has published a clear date – September 1st – until which location data for the purposes of monitoring the spread of COVID-19 is shared with the authorities.[19] Bulgaria indicates it will store data "for the length of the state of emergency" or at least 6 months.[20] Overall, available information in regards to the details of data processing is still limited. Most importantly, the European Data Protection Supervisor (EDPS) has stressed that processing of data should be transparent, temporary in nature, and limited by purpose.[21]

Even though our threat – COVID-19 – is invisible, measures can and should preferably be transparent. Without transparency, the oversight is undermined, the possibility to review the standards of cooperation is limited, and trust in the government is challenged.[22]

In order to increase transparency, aggregated location data may potentially be shared with the public. An example is Google's 'COVID-19 Community Mobility Report', which provides open-source data on the changes in people's behavior since February 16th per country (see the report of the Netherlands in Figure 1, which was cited in an RIVM briefing to the Dutch Parliament).[23]

Figure 1: Google's 'COVID-19 Community Mobility Reports' – data for the Netherlands from February 16th to April 5th, 2020

[16] "Regulation (EU) 2016/678 of the European Parliament and of the Council (General Data Protection Regulation)" recital 26.

[17] "De Block en De Backer richten."

[18] "Hilft Das Handy Im Kampf Gegen Corona?"

[19] "Vodafone Group's Five-Point Plan to Help Counter the Impact of COVID-19."

[20] Николов, "Полицията получи безконтролен достъп до телефони и интернет връзки."

[21] Wiewiórowski, "EU Digital Solidarity: A Call for a Pan-European Approach against the Pandemic."

[22] "COVID-19, Digital Surveillance and the Threat to Your Rights," 19.

[23] "COVID-19 Community Mobility Reports" Available at https://www.gstatic.com/covid19/mobility/2020-04-05_NL_Mobility_Report_en.pdf (accessed April 14, 2020).

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

Amongst European telecoms, Latvian LMT and the company Invenium (which cooperates with Austrian telecom A1) have followed this example and made their insights from location data publicly available (see the stay-at-homes rates for Austria in Figure 2).[24] As Invenium explains, their decision to share data publicly was prompted by growing external interest and the need to not only say but also *prove* that data is "anonymized, at municipality-level without traceability to individuals, in accordance with the strict data protection regulations".[25]

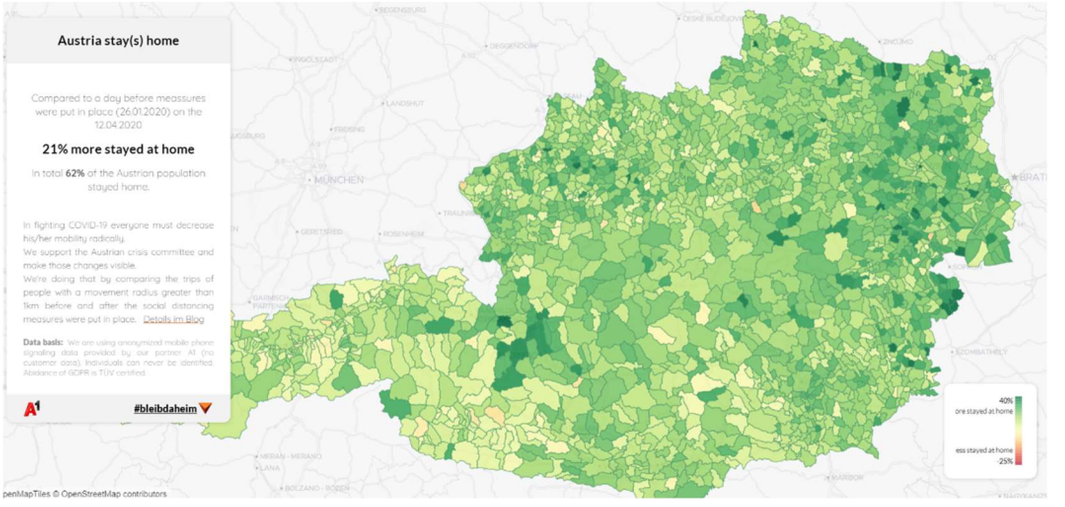

Figure 2: The proportion of anonymized mobile phone data within Austria that shows the percentage change in stay-at-homes as of 12.04.2020 (Source: Invenium)

The above-mentioned examples improve transparency. Publicly available location data invites scientists and academics to observe the ongoing efforts. It supports the public in gaining credible sources of data and dilutes disinformation. Sharing data publicly may thus contribute to a collective sense of responsibility. In a self-governed democratic society, such an approach is critical to ensure that governmental measures are trusted and conformed to.

1.3 Effectiveness

Whether chosen technological solutions can be considered proportional depends on the balance between the "means used and the intended aim (or result reached)".[26] Thus, one more crucial question remains – whether the use of anonymized phone location data is an effective measure in the fight against the COVID-19 outbreak.

First, the principal purpose of using anonymized phone location data is to monitor movements of the population and to observe the effects of lockdown measures. Telecoms argue that such data provides "accurate statistics about people's movements",

[24] "Mobile Network Research Suggests People Leave Cities to Weather the Crisis"; "Austria Stays Home" Available at https://bleibdaheim.invenium.io/en/dashboard/ (accessed April 14, 2020).

[25] "Austria Stays Home."

[26] Wiewiórowski, "EU Digital Solidarity: A Call for a Pan-European Approach against the Pandemic."

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

including the density and direction of movement.[27] Indeed, almost immediately Orange was able to report the outflux of about 17% of the Parisians away from the French capital and an increase of about 10% of the population size in the nearby province of Yonne.[28] Similarly, telecom LMT reported an increased activity in the suburban regions and a decreased activity in the Latvian capital, Riga.[29] It should, however, be understood that the accuracy (and thus effectiveness) of location data depends to a great extent on the area (urban versus rural), density of antennas, and the availability of other GSM protocol techniques – accuracy may vary from 10m to several kilometers.[30]

Second, identifying the movement of the population aids the development of informed policy, for example, to anticipate a peak of the pandemic, to adjust and scale back lockdown measures, or to redirect medical equipment to a crowded region.[31] In Italy, the government has strengthened the lockdown measures upon reports from telecoms that people were not following the initial restrictions sufficiently.[32] The Belgian government has kept existing measures in place after confirming that citizens spent more than 80% of their time in their home zip code.[33]

Third, with enough frequency and granularity, anonymized location data can provide knowledge of crowded places to law enforcement agencies in order to prevent large gatherings. The Latvian LMT telecom has confirmed the use of shared data for such purposes.[34] However, it is questionable whether this use can be securely implemented, as the Financial Times points out that aggregating data to anonymize the findings takes between 24 and 48 hours before it can be used by law enforcement agencies.[35] French authorities have argued that the use of drones is a more effective measure, as it reaches distant locations faster and transmits alert messages through loudspeakers.[36] Even where the use of drones is seemingly more effective, it raises additional privacy and proportionality concerns regarding the storage of video content and the use of facial recognition software, among others.

The above-listed applications reveal that data shared by the telecoms is of added value to the governments' ability to respond to the spread of the virus.[37] Further studies are required to understand how the access to phone location data has affected policy-

[27] "Why Is (Big) Phone Data so Valuable in Combatting the COVID-19 Pandemic?"

[28] "Why Is (Big) Phone Data so Valuable in Combatting the COVID-19 Pandemic?"

[29] "Mobile Network Research Suggests People Leave Cities to Weather the Crisis."

[30] Klimburg et al., "Pandemic Mitigation in the Digital Age," 7.

[31] Oliver et al., "Mobile Phone Data and COVID-19: Missing an Opportunity?"

[32] Hsu, "Coronavirus Pandemic Prompts Privacy-Conscious Europe to Collect Phone Data."

[33] Hsu.

[34] "Mobile Network Research Suggests People Leave Cities to Weather the Crisis."

[35] Espinoza and Fildes, "Tracking Coronavirus: Big Data and the Challenge to Privacy."

[36] Bourdon and Moynihan, "One of the Largest Cities in France Is Using Drones to Enforce the Country's Lockdown after the Mayor Worried Residents Weren't Taking Containment Measures Seriously."

[37] Mascini, "EU Expert on European Response to Virus."

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

making and whether governments at the time possessed adequate tooling and capacity to analyze provided data.[38]

In order to improve the effectiveness of collected data, it is recommended to unite efforts within the European Union under the so-called "Data for the Common Good" approach.[39] On the 8th of April, a month after major steps were taken by Member States, the European Commission issued a statement to promote "a European coordinated approach".[40] The approach is supplemented by the Commission's ongoing cooperation with "Vodafone, Deutsche Telekom, Orange and five other telecoms".[41] Collected location data is used by the Joint Research Centre (JRC) to model the spread of the virus, is not shared with third parties, and is stored only for the (undefined) duration of the crisis.[42] The measures implemented by the Commission, if acted upon in a timely manner, can further increase the value of shared data since there are more resources and scientists at the disposal of all European countries combined than in each one individually.

The current use of phone location data has aided the understanding of macro trends of people's behavior. While quarantine and social distancing measures are being monitored, some have argued that "the key to success" lies with large-scale testing and contact tracing.[43] Racing to meet the demand and to adequately respond to the COVID-19 outbreak, governments are turning to new digital solutions.

2. The second wave: contact tracing apps

At the end of March, a second wave of Europe's technological solutions began with the development of contact tracing applications.

In Germany, a GeoHealth app is meant to use a combination of GPS data, wireless networks, and Bluetooth connections to store location history.[44] In Poland, the government is investing in the contact tracing ProteGo app.[45] Other projects are ongoing in the Netherlands, Austria, Spain, Ireland, and Croatia.[46] One of the efforts to

[38] Preliminary study reveals that some public authorities lack the capacity to adequately and timely translate the findings from mobility reports to health-related conclusions, are under-staffed, or lack a necessary technological equipment Oliver et al., "Mobile Phone Data and COVID-19: Missing an Opportunity?"

[39] Klimburg et al., "Pandemic Mitigation in the Digital Age," 3.

[40] "Coronavirus: Commission Adopts Recommendation to Support."

[41] Chee, "Vodafone, Deutsche Telekom, 6 Other Telcos to Help EU Track Virus."

[42] "Coronavirus: Commission Adopts Recommendation to Support."

[43] Cohen and Kupferschmidt, "Mass Testing, School Closings, Lockdowns: Countries Pick Tactics in 'War' against Coronavirus."

[44] Schaer, "Coronavirus: They Want to Use Your Location Data to Fight Pandemic. That's a Big Privacy Issue."

[45] "Aplikacja Ministerstwa Cyfryzacji Pomoże Zahamować Rozprzestrzenianie Się Koronawirusa?" This is on top of already employed Home Quarantine app.

[46] Chee, "EU Privacy Watchdog Calls for Pan-European Mobile App for Virus Tracking"; "Dutch See Apps as Key to Relaxing Lockdown, Tracing Corona Cases"; Knolle, "Austria Bets on Mass Testing to Manage Coronavirus Spread."

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

unify the European approach is led by a coalition of academics, the Pan-European Privacy Preserving Proximity Tracing (PEPP-PT).[47]

2.1 Privacy

The PEPP-PT coalition has set leading examples of privacy-friendly contact tracing apps.[48] The coalition proposes the use of matching Bluetooth signals, based on the Singaporean "TraceTogether" app.[49] This technique broadcasts "a temporarily valid, authenticated and anonymous identifier (ID)" which is recorded in "the encrypted proximity history stored locally on a phone".[50] When one person in the network is reportedly infected, alert messages are sent to others that are stored in their phone's history using only a Bluetooth ID.[51] Collected IDs are to be stored for no longer than 21 days.[52]

Commentators argue that the Bluetooth-matching method is the "least intrusive" from available mobile tracing technologies.[53] The European Data Protection Supervisor has expressed his support for the development of apps that use Bluetooth technology and ensured that such temporary measures "seem to be a useful path to achieve privacy and personal data protection effectively".[54] Described measures show that "health protection and data protection do not have to be played off against each other even in this crisis".[55]

Importantly, as highlighted by the European Commission, the use of the app should be voluntary.[56] Choosing not to use the app may not adversely affect access to third parties' services, such as shopping malls, public transportation, or workplaces.[57]

2.2 Transparency

The development of contact tracing apps is ongoing, and the assessment of their transparency will only be possible after their full implementation. So far, a number of ongoing projects have shared the code with the GitHub community, for example the Polish app ProteGo.[58] The apps should clearly state the limited duration of processing of data, whether no other data than the Bluetooth ID is collected, and whether data is not shared with authorities but stored locally, et cetera. Overall, available information

---

[47] Chee, "EU Privacy Watchdog Calls for Pan-European Mobile App for Virus Tracking"; Espinoza and Fildes, "Tracking Coronavirus: Big Data and the Challenge to Privacy."

[48] Chee, "EU Privacy Watchdog Calls for Pan-European Mobile App for Virus Tracking."

[49] "Overview: How we Preserve Privacy and Maintain Security."

[50] "Overview: How we Preserve Privacy and Maintain Security."

[51] Mascini, "EU Expert on European Response to Virus."

[52] "Overview: How we Preserve Privacy and Maintain Security."

[53] Murphy, "US and Europe Race to Develop 'Contact Tracing' Apps."

[54] Wiewiórowski, "EU Digital Solidarity: A Call for a Pan-European Approach against the Pandemic."

[55] Becker and Feld, "Mit Bluetooth Und Datenschutz Gegen Die Pandemie."

[56] Lomas, "Digital Mapping of Coronavirus Contacts."

[57] "An Open Letter to the Members of the Wassenaar Arrangement."

[58] See https://github.com/ProteGO-app.

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

in regard to the contact tracing apps and their privacy is at this moment limited, but a tendency exists amongst public institutions and companies to provide transparency.

2.3 Effectiveness

The current contact tracing mechanism relies heavily on the memory of an infected person, the time and investigation capabilities of the medical personnel, and the ability to reach contact with indicated individuals. The main advantage of using contact tracing apps is a possibility to provide more reliable and speedy contact trace history. Analysis suggests that "about half of transmissions occur in the early phase of the infection".[59] Thus, using contact tracing apps to immediately inform potentially infected individuals to stay quarantined may significantly limit the spread of the virus.[60]

However, this premise is undermined by numerous challenges to achieve effectiveness.

First, the app must be implemented on a wide scale. At least 60% to 75% of the population must activate the app on their phones to meet the required threshold.[61] Reaching such a high percentage of use will be challenging. Many people may choose not to download the app, not have enough storage, may be unable to use the app due to dated mobile phone versions, may have insufficient battery power to support constant Bluetooth activation, kids and senior citizens (in the highest-risk group) may not be carrying or even own a personal smart device. In Singapore, two weeks after launching, the use of the app was still significantly under the necessary threshold at about 12%.[62]

To meet the desired effectiveness, a political discussion emerged in the Netherlands in which politicians considered mandatory implementation of an app.[63] However, such a measure is widely rejected.[64] Governments will have to employ creative measures to spark a common social responsibility and inspire people to use the apps. Greater transparency is one of the approaches to raise trust in proposed technological solutions.

Second, even if the use of the contact tracing apps is widespread, its effectiveness is still not guaranteed. The apps can "contribute towards protecting health services, supporting vulnerable people and simultaneously gradually releasing communities out of extended quarantine" *if* combined with a widespread availability of testing, social distancing, and quarantine measures.[65] The effectiveness depends on a long chain of uncertain events. After having tested positive, individuals need to provide reliable input

---

[59] "Controlling Coronavirus Using a Mobile App to Trace Close Proximity Contacts."

[60] "Controlling Coronavirus Using a Mobile App to Trace Close Proximity Contacts."

[61] Macon-Cooney, "Contact Tracing and the Fight Against Covid-19: How Digital Tools Can Help"; "Controlling Coronavirus Using a Mobile App to Trace Close Proximity Contacts."

[62] Macon-Cooney, "Contact Tracing and the Fight Against Covid-19: How Digital Tools Can Help"; Newton, "Why Bluetooth Apps Are Bad at Discovering New Cases of COVID-19."

[63] Verhagen, "De Overheid Wil Een Privacyvriendelijke Pandemie-App Voor Alle Nederlanders, Maar Hoe Dan?"

[64] "AP"; "An Open Letter to the Members of the Wassenaar Arrangement."

[65] Muller et al., "Een Brief Aan de Premier Mark Rutte Inzake: COVID-19 Tracking- En Tracingapp En Gezondheidsapp," April 13, 2020; "Controlling Coronavirus Using a Mobile App to Trace Close Proximity Contacts."

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

of their health status and test results immediately. Then, on the opposite side, individuals that receive a warning must stay home (if they have symptoms) or be tested (if they have no symptoms). The conclusion is that having coronavirus tests available and applied promptly to confirm the hypothetical infection is critical to maximize any app's effectiveness.

Third, on top of the practical issues, the social impact of the contact tracing apps may not be overlooked. In a letter to the Dutch prime minister, academics point out that the deployment of contact tracing apps may create a 'false sense of security', leading people to take less strict measures and to be biased to trust the app's (false) reliability.[66] Limited reliability of the app means that the app may identify "false positives" or "false negatives" and lead to inefficient policies.[67] With possible technical issues or incorrect Bluetooth tracing results, the use of contact tracing apps may consequently undermine society's trust in the government.

Lastly, in order to ensure that implemented measures are effective, it is recommended that governments, and the European Union itself, coordinate united efforts. With many private companies developing their own apps, including Apple and Google, the measures are becoming dispersed. The European Data Protection Supervisor calls for the apps to be a coordinated effort and the PEPP-PT coalition highlights the need for "international interoperability" to ensure that contact tracing continues when crossing borders within the EU.[68]

The use of contact tracing apps marks a significant change in the approach to dealing with quarantine in times of an epidemic. For centuries, people have used non-digital means to mark people that are infected, submitting them to public shaming to limit their public appearance. In 16th century London, houses of plague victims were marked with blue crosses.[69] Even today, in India the hands of infected individuals are marked with indelible ink.[70] The digital means used in China, where green, yellow, and red QR codes are shown on a phone to access buildings, enter public transportation, and buy groceries, can be considered the use of a similar old-school approach to cast out those who are infected.[71] Contact tracing apps promise to improve accuracy and effectiveness of contact tracing and, most of all, to empower citizens in protecting their health.[72]

Nevertheless, the use of the contact tracing apps should be implemented when the mean is supported by "intended aim". At the moment, there are reasonable concerns

---

[66] Muller et al., "Een Brief Aan de Premier Mark Rutte Inzake: COVID-19 Tracking- En Tracingapp En Gezondheidsapp," April 13, 2020.

[67] Muller et al.

[68] "Overview: How we Preserve Privacy and Maintain Security"; Wiewiórowski, "EU Digital Solidarity: A Call for a Pan-European Approach against the Pandemic."

[69] Nuttall, "Digital Lockdown."

[70] Koper and Busvine, "In Europe, Tech Battle against Coronavirus Clashes with Privacy Culture."

[71] Mazur, Zhong, and Krolik, "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags - The New York Times."

[72] Harari, "Yuval Noah Harari: The World after Coronavirus."

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

that the effectiveness of second wave solutions is undermined by a lack of widespread implementation, insufficient logistical support in terms of available testing, undermined social responsibility, and a 'false sense of security'.

Conclusions

In this paper, two waves of technological solutions are identified and evaluated to clarify the main trends in privacy, transparency, and effectiveness.

Notably, the review of implemented (first-wave) and proposed (second-wave) measures suggests that both governments and companies are aware of the privacy concerns. Telecom providers ensure that data is shared in compliance with privacy protection laws by aggregating anonymized data. Likewise, the PEPP-PT supports only the development of contact tracing apps that use Bluetooth signals to provide anonymous data storage. Privacy protection authorities all around Europe have been involved in the process and continue to oversee compliance with data protection safeguards. This approach follows European privacy protection standards and sets an unmatched example on the international stage.

In order to improve trust in implemented measures, European governments should continue to promote greater transparency. As shown with the review of first-wave measures, citizens are assured that privacy-safeguards are implemented but are to a great extent unable to check the details of business-to-government arrangements. The first wave also lacked common EU guiding principles. With the first steps taken into the second wave, the EU has taken more agency to lead towards more transparent and principles-based methods.

Initial findings prove that the use of phone location data during the COVID-19 pandemic is an effective measure to inform policymaking. The use of contact tracing apps, on the contrary, is largely unprecedented. The apps are being designed to not only *inform* about the spread of the virus, but also to *prevent* its expansion by limiting the circle of infection. However, a long list of requirements (widespread use of the app, reliable use, available testing, etc.) will have to be met for the app to be effective in informing about or preventing the spread of the virus. If contact tracing apps are implemented in Europe, it should be observed whether their use aids the prevention of COVID-19 and what area their effects on healthcare, political decision-making, and also the social sphere. The results of this experiment will be crucial to the setting of standards for the use of technology in future virus outbreaks.

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

Bibliography

Álvarez-Pallete, José María. "Telefónica Announces Measures Related to COVID-19." Telefonica, March 10, 2020. https://www.telefonica.com/en/web/press-office/-/telefonica-announces-measures-related-to-covid-19.

"An Open Letter to the Members of the Wassenaar Arrangement." Amnesty International, February 12, 2014.

Autoriteit Persoonsgegevens. "AP: Corona Apps Alleen Als Privacy Gewaarborgd Is," April 8, 2020. https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-corona-apps-alleen-als-privacy-gewaarborgd.

CyberDefense24. "Aplikacja Ministerstwa Cyfryzacji Pomoże Zahamować Rozprzestrzenianie Się Koronawirusa?," April 6, 2020. https://www.cyberdefence24.pl/aplikacja-ministerstwa-cyfryzacji-pomoze-zahamowac-rozprzestrzenianie-sie-koronawirusa.

Invenium Data Insights GmbH. "Austria Stays Home," February 4, 2020. www.invenium.io.

Becker, Kristin, and Christian Feld. "Handys in Der Corona-Krise: Mit Bluetooth Und Datenschutz Gegen Die Pandemie." tagesschau.de, January 4, 2020. https://www.tagesschau.de/inland/coronavirus-handydaten-101.html.

Bourdon, Megan, and Ruqayyah Moynihan. "One of the Largest Cities in France Is Using Drones to Enforce the Country's Lockdown after the Mayor Worried Residents Weren't Taking Containment Measures Seriously." Business Insider, March 20, 2020. https://www.businessinsider.com/coronavirus-drones-france-covid-19-epidemic-pandemic-outbreak-virus-containment-2020-3.

C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (The Court of Justice of the European Union May 13, 2014).

C-362/14 Maximillian Schrems v Data Protection Commissioner (The Court of Justice of the European Union October 6, 2015).

Chee, Foo Yun. "EU Privacy Watchdog Calls for Pan-European Mobile App for Virus Tracking." *Reuters*, April 6, 2020. https://www.reuters.com/article/us-health-coronavirus-tech-privacy-idUSKBN21O1KJ.

———. "Vodafone, Deutsche Telekom, 6 Other Telcos to Help EU Track Virus." *Reuters*, March 25, 2020. https://www.reuters.com/article/us-health-coronavirus-telecoms-eu-idUSKBN21C36G.

Cohen, Jon, and Kai Kupferschmidt. "Mass Testing, School Closings, Lockdowns: Countries Pick Tactics in 'War' against Coronavirus." AAAS, March 18, 2020. https://www.sciencemag.org/news/2020/03/mass-testing-school-closings-lockdowns-countries-pick-tactics-war-against-coronavirus.

University of Oxford. "Controlling Coronavirus Using a Mobile App to Trace Close Proximity Contacts," April 2, 2020. http://www.ox.ac.uk/news/2020-04-02-controlling-coronavirus-using-mobile-app-trace-close-proximity-contacts.

European Commission. "Coronavirus: Commission Adopts Recommendation to Support." Text, April 8, 2020. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_626.

Google. "COVID-19 Community Mobility Reports," n.d. https://www.google.com/covid19/mobility/.

Amnesty International. "COVID-19, Digital Surveillance and the Threat to Your Rights," April 3, 2020. https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/.

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

"De Block en De Backer richten." Accessed April 6, 2020. https://www.medisfeer.be/nl/nieuws/de-block-en-de-backer-richten-data-against-corona-taskforce-op.html.

DutchNews.nl. "Dutch See Apps as Key to Relaxing Lockdown, Tracing Corona Cases," April 7, 2020. https://www.dutchnews.nl/news/2020/04/dutch-see-apps-as-key-to-relaxing-lockdown-tracing-corona-suspects/.

Espinoza, Javier, and Nic Fildes. "Tracking Coronavirus: Big Data and the Challenge to Privacy." The Financial Times, April 8, 2020. https://www.ft.com/content/7cfad020-78c4-11ea-9840-1b8019d9a987.

Harari, Yuval Noah. "Yuval Noah Harari: The World after Coronavirus." Financial Times, March 20, 2020. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75.

tagesschau.de. "Hilft Das Handy Im Kampf Gegen Corona?," March 29, 2020. https://www.tagesschau.de/inland/handy-coronavirus-101.html.

Hsu, Jeremy. "Coronavirus Pandemic Prompts Privacy-Conscious Europe to Collect Phone Data." IEEE Spectrum, April 3, 2020. https://spectrum.ieee.org/tech-talk/telecom/security/how-coronavirus-pandemic-europe-collecting-phone-data.

Jegelevičius, Linas. "Lithuania Puts COVID-19-Related Prosecution above Human Rights." Baltic News Network, April 2, 2020. https://bnn-news.com/lithuania-puts-covid-19-related-prosecution-above-human-rights-212024.

Klimburg, Alexander, Louk Faesen, Paul Verhagen, and Philipp Mirtl. "Pandemic Mitigation in the Digital Age: Digital Epidemiological Measures to Combat the Coronavirus Pandemic." The Hague Centre for Strategic Studies, March 28, 2020. https://hcss.nl/sites/default/files/files/reports/Pandemic%20Mitigation%20Measures%20in%20the%20Digital%20Age%20-%20Final.pdf.

Knolle, Kirsti. "Austria Bets on Mass Testing to Manage Coronavirus Spread." *Reuters*, March 24, 2020. https://www.reuters.com/article/us-health-coronavirus-austria-idUSKBN21B1DH.

Koper, Anna, and Douglas Busvine. "In Europe, Tech Battle against Coronavirus Clashes with Privacy Culture." *Reuters*, March 26, 2020. https://www.reuters.com/article/us-health-coronavirus-europe-tech-poland-idUSKBN21D1CC.

Lomas, Natasha. "Digital Mapping of Coronavirus Contacts Will Have Key Role in Lifting Europe's Lockdown, Says Commission." *TechCrunch* (blog), April 15, 2020. https://social.techcrunch.com/2020/04/15/digital-mapping-of-coronavirus-contacts-will-have-key-role-in-lifting-europes-lockdown-says-commission/.

Macon-Cooney, Benedict. "Contact Tracing and the Fight Against Covid-19: How Digital Tools Can Help." Institute for Global Change, April 6, 2020. https://institute.global/policy/contact-tracing-and-fight-against-covid-19-how-digital-tools-can-help.

Mascini, Lucette. "EU Expert on European Response to Virus: 'Telecom Data for Tracking Corona Can Be Made Anonymous.'" *Innovation Origins* (blog), April 11, 2020. https://innovationorigins.com/eu-expert-on-european-response-to-virus-telecom-data-for-tracking-corona-can-be-made-anonymous/.

Mazur, Paul, Raymond Zhong, and Aaron Krolik. "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags - The New York Times." The New York Times, March 1, 2020. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

LSM.LV. "Mobile Network Research Suggests People Leave Cities to Weather the Crisis," April 3, 2020. https://eng.lsm.lv/article/economy/economy/mobile-network-research-suggests-people-leave-cities-to-weather-the-crisis.a354551/.

Moné, Brianna. "10 Countries Are Now Tracking Phone Data as the Coronavirus Pandemic Heralds a Massive Increase in Surveillance." Business Insider, March 21, 2020. https://www.businessinsider.nl/countries-tracking-citizens-phones-coronavirus-2020-3?international=true&r=US.

Moné, Brianna, Dave Mosher, and Aylin Woodward. "A comprehensive timeline of the new coronavirus pandemic, from China's first COVID-19 case to the present." Business Insider, March 24, 2020. https://www.businessinsider.com/coronavirus-pandemic-timeline-history-major-events-2020-3.

Muller, Catelijne, Natali Helberger, Virginia Dignum, and Frank Dignum. "Een Brief Aan de Premier Mark Rutte Inzake: COVID-19 Tracking- En Tracingapp En Gezondheidsapp," April 13, 2020. https://www.engineersonline.nl/download/Brief-Minister-President-Rutte-Ministers-De-Jonge-Van-Rijn-Grapperhaus-de-heer-Sijbesma-inzake-COVID-19-tracking-en-tracing-en-gezondheidsapps.pdf.

Murphy, Hannah. "US and Europe Race to Develop 'Contact Tracing' Apps." *Financial Times*, April 3, 2020. https://www.ft.com/content/d42acff2-b0b5-400b-b38f-ec621d4efd95.

Newton, Casey. "Why Bluetooth Apps Are Bad at Discovering New Cases of COVID-19." The Verge, April 10, 2020. https://www.theverge.com/interface/2020/4/10/21215267/covid-19-contact-tracing-apps-bluetooth-coronavirus-flaws-public-health.

Nuttall, Clare. "Digital Lockdown." intellinews.com, April 8, 2020. http://www.intellinews.com/digital-lockdown-180258/.

Oliver, Nuria, Emmanuel Letouze, Harald Sterly, Sebastien Delataille, Marco De Nadai, Bruno Lepri, Renaud Lambiotte, Richard Benjamins, Ciro Cattuto, and Vittoria Colizza. "Mobile Phone Data and COVID-19: Missing an Opportunity?" *Arxiv*, March 26, 2020. https://arxiv.org/ftp/arxiv/papers/2003/2003.12347.pdf.

PEPP-PT. "Overview: How we Preserve Privacy and Maintain Security." Accessed April 9, 2020. https://www.pepp-pt.org.

"Regulation (EU) 2016/678 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)." Official Journal of the European Union, April 29, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Reidy, Pádraig. "After Edward Snowden's Revelations about the NSA, What Is the EU Doing." *The Independent*, September 25, 2013, sec. Comment. http://www.independent.co.uk/voices/comment/after-edward-snowdens-revelations-about-the-nsa-what-is-the-eu-doing-to-ensure-our-online-privacy-8839424.html.

Schaer, Cathrin. "Coronavirus: They Want to Use Your Location Data to Fight Pandemic. That's a Big Privacy Issue." ZDNet, March 19, 2020. https://www.zdnet.com/article/coronavirus-they-want-to-use-your-location-data-to-fight-pandemic-thats-a-big-privacy-issue/.

Stupp, Catherine. "Europe Tracks Residents' Phones for Coronavirus Research." *Wall Street Journal*, March 27, 2020, sec. WSJ Pro.

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms

https://www.wsj.com/articles/europe-tracks-residents-phones-for-coronavirus-research-11585301401.

Verhagen, Laurens. "De Overheid Wil Een Privacyvriendelijke Pandemie-App Voor Alle Nederlanders, Maar Hoe Dan?" *De Volkskrant*, April 8, 2020, sec. Nieuws & Achtergrond. https://www.volkskrant.nl/gs-b83e5e5e.

Verseck, Keno. "Coronavirus: Rule of Law under Attack in Southeast Europe." DW.COM, March 24, 2020. https://www.dw.com/en/coronavirus-rule-of-law-under-attack-in-southeast-europe/a-52905150.

Vodafone. "Vodafone Group's Five-Point Plan to Help Counter the Impact of COVID-19," April 2020. https://www.vodafone.com/covid19.

World Health Organization. "WHO Director-General's Statement on IHR Emergency Committee on Novel Coronavirus (2019-NCoV)," January 30, 2020. https://www.who.int/dg/speeches/detail/who-director-general-s-statement-on-ihr-emergency-committee-on-novel-coronavirus-(2019-ncov).

Orange. "Why Is (Big) Phone Data so Valuable in Combatting the COVID-19 Pandemic?," April 2020. https://www.orange.com/en/news/2020/April/Why-is-big-phone-data-so-valuable-in-combatting-the-COVID-19-pandemic.

Wiewiórowski, Wojciech. "EU Digital Solidarity: A Call for a Pan-European Approach against the Pandemic." *European Data Protection Supervisor*, April 6, 2020.

Wright, Helen. "Statistics Estonia to Study People's Movements during Emergency Situation." ERR, March 24, 2020. https://news.err.ee/1068209/statistics-estonia-to-study-people-s-movements-during-emergency-situation.

Николов, Красен. "Полицията получи безконтролен достъп до телефони и интернет връзки." Mediapool.bg, March 14, 2020. https://www.mediapool.bg/politsiyata-poluchi-bezkontrolen-dostap-do-telefoni-i-internet-vrazki-news305118.html.

This content downloaded from
117.103.83.94 on Sat, 11 Jul 2020 14:02:29 UTC
All use subject to https://about.jstor.org/terms