ETUI Policy Brief

European Economic, Employment and Social Policy

N°5/2020

Covid-19 impact series

COVID-19 contact-tracing apps: how to prevent privacy from becoming the next victim

Aída Ponce Del Castillo

Aída Ponce Del Castillo is a Senior Researcher at the European Trade Union Institute in Brussels, Belgium.

Key points

- **Using contact-tracing apps to fight the spread of COVID-19 is intrusive and threatens EU citizens' right to privacy. To defend this right, key rules and principles of EU law, in particular those embedded in the General Data Protection Regulation (GDPR) and e-Privacy Directive, must be upheld.**
- **Claiming that defending privacy undermines the fight against the pandemic and the reopening of the economy is a mistake: for contact-tracing apps to be at all effective, they must be voluntarily and freely downloaded and used by a majority of citizens. This will only happen if citizens are confident that their privacy is not at stake. The two battles, for privacy and against COVID-19, are complementary, not opposed.**
- **Contact-tracing apps should only be used in the workplace if specific requirements are met (regarding, among other things, the purpose of the app, the type of data collected, how long the data is kept, whether workers give their consent, and whether trade unions are involved).**
- **Finally, it is of the utmost importance that contact-tracing apps are not used to sow the seeds of a future culture of hyper-surveillance in the workplace.**

Introduction

The COVID-19 pandemic is far from over and the number of victims will unfortunately continue to rise. However, in the second week of April 2020, several Member States of the European Union (EU) such as Austria, Spain and Denmark, among others, started loosening their lockdowns. Other countries will begin to do the same at the beginning of May.

In parallel, tracing apps have increasingly been mentioned as useful tools to accompany and contribute to a return to normality, despite the many ethical and legal questions they raise. On 14 April, the UK revealed it would release an app to track people reporting COVID-19 symptoms and to alert people they were in contact with. On 10 April, Apple and Google (2020a) announced they would partner and launch 'a comprehensive solution that includes application programming interfaces (APIs) and operating system-level technology to assist in enabling contact tracing'. On 21 April, Dutch Prime Minister Mark Rutte said that the development of COVID-19 tracing apps would continue, despite testing seven of them and finding out that they all failed to meet the requirements for security, privacy and reliability.

The pressure exerted by business circles and lobbies to restart and 'save the economy' has been intense. What started as a public health crisis morphed into an economic crisis and we are now faced with a 'trick-or-treat' choice: accept to 'pay the price' and use invasive tracing apps, and by so doing facilitate a gradual reopening of business, or fight for privacy and delay the return to normality.

We need to reject this binary choice. Defending privacy does not undermine the restart of the economy: for contact-tracing apps to be at all effective, they must be voluntarily and freely downloaded and used by a majority of citizens. This will only happen if citizens are confident their privacy is not at stake. That may be the difference between a limited number of people using apps, which would make them useless, and mass use, the first step towards ensuring their effectiveness.

etui.

Losing our privacy rights cannot be the price we have to pay to restart the economy. This policy brief presents several key requirements which should help us to achieve that, both as citizens and in our workplaces.

Multiple apps, multiple technological approaches, multiple privacy issues

Faced with the inevitable deployment of tracing technology in the fight against COVID-19, we have to make a choice. Are we willing to live in a 'COVID-1984' world, under an authoritarian, Orwellian surveillance system, with across-the-board tracing of citizens and the end of privacy? Do we start using apps developed by private corporations who will ask us to trust them and to share with them personal and location data? Or do we call for a common EU approach and an app based on GDPR rules including privacy-by-design that will both help to fight the spread of the virus and protect people's privacy?

Apps are currently developed with very little or no coordination and very diverse approaches: some collect anonymised, aggregated data to monitor population movements, to enforce lockdowns, or to collect statistical data; others focus on self-assessment. More recent efforts have zeroed in on contact-tracing apps, that locate and trace infected patients, possibly infected persons and the individuals they have been in contact with.

All suffer from serious shortcomings: they are invasive; as early warning tools they only work if a significant number of people install and activate the app; they can create unnecessary alarm or confusion by generating false positives. Worse, they are not always reliable. Firstly, Bluetooth signal travels further in open spaces than in urban environments, meaning it can give false positives or false negatives. Furthermore, one can be a few metres away from someone and not be at risk, for example if the signal 'pings' someone who is standing on the other side of a wall, while a metro seat can potentially remain a virus 'hotspot' for several hours.

The most glaring shortcoming of these apps is related to privacy. Technology and emergency legislation can help to contain or limit the COVID-19 crisis, but there is a need to have a democratic discussion about the rapid deployment of technology solutions that seem to override fundamental rights, including social dialogue as well as information, consultation and participation rights. The adoption of these technologies poses serious new issues and risks in the context of privacy and data protection.

Around the world, some extreme solutions have been implemented. The Singapore COVID-19 Dashboard, for example, shares information about every infected individual, including their ethnic origin, age, gender, and in some cases where they live, where they work, the hospital they are in and who they may have infected (https://co.vid19.sg/singapore/). Equally unacceptable are the solutions that create the risk of confidential patient data being shared with US technology businesses. On 12 April, Lewis *et al.* (2020) revealed that Palantir, a US big data firm, and Faculty, a British artificial intelligence start-up, are involved in a data-mining operation launched by the UK government, which involves storing sensitive and confidential health information in a central database, including the content of people's calls to the UK National Health Service helpline.

Given the multiplicity of apps and technological approaches developed globally to address the COVID-19 crisis, the ETUI is creating a map of COVID-19 containment initiatives (available online at www.etui.org), building on work done by gdprhub.eu and other sources, which will be updated on a regular basis.

This policy brief also presents four technology use cases: the Self-Quarantine Safety Protection app of South Korea, the TraceTogether app of Singapore, the recent joint Apple and Google initiative and the Pan-European Privacy-Preserving Proximity-Tracing Initiative. These use cases were selected because they describe four different realities: Singapore and South Korea have been held up as examples across the world for their effectiveness in containing the spread of the virus (Mesmer 2020; McCurry 2020; Leung 2020). The Apple/Google application programming interface (API) and the Pan-European Privacy-Preserving Proximity-Tracing Initiative were selected because they are joint initiatives which claim to place user privacy and security at the core of their design.

The Brief then presents a list of recommendations and requirements that contact-tracing apps need to meet in order to both be effective and ensure user privacy.

Finally, it examines the specific case of contact-tracing apps used in an employment context.

Four technology use cases

1. South Korea: the Self-Quarantine Safety Protection app

What is it and how does it work?

Developed by the Ministry of the Interior and Safety, this app uses GPS technology to monitor and track infected citizens in self-quarantine. The app allows government officials to track the location of every self-quarantined patient. In case of breach, an alert is triggered. Additionally, a communication process is established between users and officials, with patients reporting their symptoms to a local government case officer twice a day. Anyone leaving their quarantine location without permission faces up to a year imprisonment or a fine of 7,500 euros. Any foreigner who refuses to install the app or leaves the quarantine area without permission faces immediate deportation (Central Disaster and Safety Countermeasures Headquarters 2020).

Privacy features/issues

The app collects personal information, including name, date of birth, gender, nationality, mobile phone number, mobile phone number of a family member, and address where the quarantine is taking place. Interestingly, the Korea Centre for Disease Control Prevention also admits that patients are first interviewed, then: 'to fill in the areas they perhaps haven't told us, and also to verify, we use GPS data, surveillance camera footage, and credit card transactions to recreate their route a day before their symptoms showed' (BBC 2020).

2. Singapore: the TraceTogether app

What is it and how does it work?
Developed by Singapore's Government Technology Agency (under the direction of the Prime Minister) and Ministry of Health (GOVTECH Singapore 2020),, TraceTogether is an app that uses Bluetooth signals to determine whether participating mobile phones have been in contact with one another. The app, based on a protocol called BlueTrace and a codebase called OpenTrace, estimates the distance between users and the duration of the encounter. The mobile phones exchange identifiers and the app stores this history of encounters locally (on the mobile phone) for 21 days. The data is not accessible to the authorities. If someone becomes infected, they are asked to share their contact history with the health authority, which can then ensure the person is isolated (Government Technology Agency of Singapore 2020).

Privacy features/issues
The app integrates key privacy features, including local storage of the user's encounter history, temporary identifiers, and revocable consent. However, to download and set up the app, the user has to give explicit consent to participate in TraceTogether and to agree to have his/her mobile number and TraceTogether data used for contact tracing. In addition, while contact logging is decentralised (i.e. no uploading of encounters to a central database) contact tracing is centralised: in designing the app, the TraceTogether team made the fundamental choice to develop a hybrid system ('human-in-the-loop') rather than a fully decentralised system. The idea is that COVID-19 diagnoses should be confirmed by a human in order to avoid false reports of contamination, which would provoke panic. Centralised contact-tracing starts when a user's history is shared with the Ministry, whose officials then classify contacts into 'close', 'casual' and 'transient', based on proximity and duration, and then take the necessary action.

3. Apple and Google Privacy-Preserving Contact Tracing

What is it and how does it work?
Google and Apple (2020a) have announced that they want to enable the use of Bluetooth Low Energy technology to help governments and health agencies reduce the spread of COVID-19. They are not building an app but have created a simple application programming interface (API) which will enable interoperability between Android and iOS devices and make it easier for other actors to build tracing apps. Most of these apps will use Bluetooth and operate as described above (TraceTogether). The next step for Apple and Google will be to integrate the API's functionality into their operating systems (iOS and Android) (Apple 2020b).

Privacy features/issues
In this approach, Apple and Google are not launching an app but enabling others to do so. The privacy risks described above remain, in particular those associated with the centralisation of contact-tracing. Decentralising both contact-logging and tracing may be how more people will be convinced to join in, even if it increases the risk of false positives.

Indeed, adoption rates remain low and need to be above a certain threshold for the app to be effective: in Singapore, only 20% of the population has chosen to use TraceTogether. Australia estimates a tracing app would work if used by 40% (Dalzell and Probyn 2020). The UK Ministry of Health has set the threshold at around 60% of the adult population.

Apple and Google claim that 'privacy, transparency, and consent are of utmost importance'. If, as planned, the technology becomes embedded in their operating system, we could face a situation where a government, overloaded with COVID-19 cases and deaths or frustrated by the low use of their app, would no longer require citizens' consent to use it but would force them to do so.

4. The Pan-European Privacy-Preserving Proximity-Tracing Initiative (PEPP-PT)

The Pan-European Privacy-Preserving Proximity-Tracing (PEPP-PT) is a project led by an EU consortium with more than 130 members in eight European countries[1] It intends to develop and release software code that can be used by national authorities to build COVID-19 tracing apps. The approach is very similar to the TraceTogether and Apple/Google initiative, based on Bluetooth signal, with secure data anonymisation and cross-border interoperability. EU Commissioner for Internal Market and Services Thierry Breton has recently stated that the European Commission is verifying whether an app using the PEPP-PT software would truly comply with EU values.

Recommendations and key requirements for contact-tracing apps

Tracing apps must respect key rules and principles of EU law (i.e. GDPR and the e-Privacy Directive) which cover: the proportionality of the measure in terms of duration and scope, limited data retention, data minimisation, data deletion, purpose limitation, genuine anonymisation of data, and app use being voluntary and based on people opting in.

If and when contact-tracing apps are introduced, risk assessment must be carried out.

The power given to the state to trace people should be removed once the crisis is over, and an independent authority should be established to ensure the rules are implemented (and to act if they are not).

In addition, what is proposed in the 'Common EU Toolbox for Member States' published on 15 April by the eHealth Network (2020), and in the letter from the European Data Protection Board (EDPB) to the Directorate General for Justice and Consumers (EDPB 2020a) should be taken into consideration by Member States.

The recently launched European Strategy for Data should take into account the COVID-19 crisis and establish a governance framework that genuinely takes into account the data dimension

1 Those countries are Austria, Belgium, Denmark, France, Germany, Italy, Spain and Switzerland.

of the pandemic, so that the tracing of citizens does not become the 'new normal'.

Finally, building on the European Data Protection Board's statement (EDPB 2020b), the following 12 requirements need to be met:

1. Legislation must be passed before an app is rolled out, and parliamentary oversight is needed during the process.
2. The app must be created and implemented by public authorities, rather than private corporations.
3. Use of the app must be based on documented and legally established security.
4. The code should be open source and freely accessible.
5. Use of the app must be proportionate in terms of duration and scope. As stated by the EDPB, 'emergency is a legal condition which may legitimise restrictions of freedoms, provided these restrictions are proportionate and limited to the emergency period'.
6. Purpose limitation: app use should be limited to stopping the spread of COVID-19. Minimum and relevant contact data only must be collected and stored.
7. The system must be totally decentralised, with no central authority involved.
8. Data retention should be limited, and collected data must be anonymous or anonymised, encrypted and deleted after a certain amount of time.
9. The app must be free, based on voluntary use ('opt in') and removable, not embedded in the operating system of mobile phones.
10. People refusing to use it or deciding to remove it after installation should not be penalised.
11. Bluetooth identifiers must change regularly.
12. It should not be possible for location- or movement-tracking to be derived from the contact-tracing.

Contact-tracing in the employment context

Some employers have introduced what they call 'COVID solutions' for workers. In Belgium, the Port of Antwerp has launched the use of wristbands or 'proof of health' wearables, developed by technology company Rombit, to prevent coronavirus infections in its working environment (ATV 2020, Rombit 2020). This wristband works in a similar way to the mobile apps described above but without any internet connection. If workers come too close to each other, an alarm is triggered. Although Rombit's website states that 'it does not capture or store location or other privacy-sensitive data', the tool features real-time individual worker localisation and monitoring. The website states that 'any personal information is fully encrypted and kept on the Romware Platform and only accessible by the employer'.

There can be indeed a case for legitimate and proportionate use of monitoring applications in the case of workers who are in regular or frequent contact with potentially infected people: healthcare workers, home carers, public transport employees, law enforcement, first responders (including firefighters), teachers, waiters, etc. (Ellison 2020, Gamio 2020). In those cases, though, employers should still demonstrate that there is a strong reason to justify the use of contact-tracing systems at the workplace, that there is no alternative less intrusive solution and that such initiatives do not 'sow the seeds' of a culture of hyper-surveillance.

Trade unions also have a key role to play and should be involved at every step of the process. This includes assessing the risks, a necessary step before the use of an app can be envisaged. App deployment can then take place, provided it: (1) respects labour rights, (2) is negotiated with workers' representatives, (3) follows GDPR rules and (4) as well as the requirements presented above, follows the criteria below:

1. Collects personal data exclusively to prevent contagion of COVID-19, and not for other purposes.
2. Requires explicit consent from workers for processing that specific data.
3. Provides simple, clear and transparent information of how their data is going to be used.
4. Collects data that is strictly necessary to protect the health of workers, and not to pursue surveillance or for other purposes.
5. Puts in place new risk management and organisational measures in the company to evaluate the environmental and working conditions changes and to keep the data safe.
6. Sets limits to the duration of data retention.
7. Involves active participation of workers' representatives and data protection officers.

Final remarks

The COVID-19 pandemic has made the impossible a reality: tracing technology and apps are sprouting up everywhere, with no coordination, no democratic debate and very little opposition. The circumstances are exceptional and may call for exceptional measures, but these should not become the new normal. This is a real risk and the tracing of citizens and workers should and will be a key and structural priority for the European and global trade union movement.

From a legal perspective, the EU legal framework – including the GDPR and the recent 'European data strategy', which lays down the EU Commission's vision on data access, use and re-use – gives European citizens the right to protect their privacy and personal data. COVID-19 should not be allowed to threaten this right: tracing and monitoring technologies are not a magic wand that will painlessly solve the problem; they should only be used for legitimate purposes, when and if proven necessary, and with real safeguards in place.

References

Apple and Google (2020a) Apple and Google partner on COVID-19 contact tracing technology, 10 April 2020. https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology

Apple and Google (2020b) Privacy-preserving contact tracing. https://www.apple.com/covid19/contacttracing

ATV (2020) Port of Antwerp test slimme armband om coronabesmettingen op de werkvloer te voorkomen, 17 April 2020. https://atv.be/nieuws/port-of-antwerp-test-slimme-armband-om-coronabesmettingen-op-de-werkvloer-te-voorkomen

BBC (2020) Coronavirus privacy: are South Korea's alerts too revealing? 5 March 2020. https://www.bbc.com/news/world-asia-51733145

Central Disaster and Safety Countermeasures Headquarters (2020) Guide on the installation of "self-quarantine safety protection app". http://ncov.mohw.go.kr/upload/ncov/file/202004/15857327 93827_20200401181953.pdf

Dalzell S. and Probyn A. (2020) Convincing Australians to use government-sponsored coronavirus-tracing app a tough ask, ABC News, 15 April 2020. https://www.abc.net.au/news/2020-04-15/challenge-to-convince-australians-to-use-coronavirus-tracing-app/12151130

eHealth Network (2020) Mobile applications to support contact tracing in the EU's fight against COVID-19: common EU toolbox for Member States, 15 April 2020. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

Ellison J. (2020) Millions of US workers at risk of infections on the job, UW researchers calculate, emphasizing need to protect against COVID-19, UW News, 6 March 2020. https://www.washington.edu/news/2020/03/06/millions-of-us-workers-at-risk-of-infections-on-the-job-uw-researchers-calculate-emphasizing-need-to-protect-against-covid-19/

European Data Protection Board (2020a) Letter to Olivier Micol, Head of Unit European Commission, DG for Justice and Consumers, 14 April 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

European Data Protection Board (2020b) Statement on the processing of personal data in the context of the COVID-19 outbreak, adopted on 19 March 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

Gamio L. (2020) The workers who face the greatest coronavirus risk, The New York Times, 15 March 2020. https://www.nytimes.com/interactive/2020/03/15/business/economy/coronavirus-worker-risk.html

Government Technology Agency of Singapore (2020) 6 things about OpenTrace, the open-source code published by the TraceTogether team. https://www.tech.gov.sg/media/technews/six-things-about-opentrace

GOVTECH Singapore (2020) Responding to COVID-19 with Tech. https://www.tech.gov.sg/products-and-services/responding-to-covid-19-with-tech/

Knight W. (2020) How AI is tracking the coronavirus outbreak, Wired, 8 February 2020. https://www.wired.com/story/how-ai-tracking-coronavirus-outbreak/

Leung H. (2020) Why Singapore, once a model for coronavirus response, lost control of its outbreak, Time, 20 April 2020. https://time.com/5824039/singapore-outbreak-migrant-workers/

Lewis P., Conn D. and Pegg D. (2020) UK government using confidential patient data in coronavirus response, The Guardian, 12 April 2020. https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response

Manancourt V. (2020) Coronavirus tests Europe's resolve on privacy, Politico, 10 March 2020. https://www.politico.eu/article/coronavirus-tests-europe-resolve-on-privacy-tracking-apps-germany-italy/

McCurry J. (2020) Test, trace, contain: how South Korea flattened its coronavirus curve, The Guardian, 23 April 2020. https://www.theguardian.com/world/2020/apr/23/test-trace-contain-how-south-korea-flattened-its-coronavirus-curve

Mesmer P. (2020) Endiguer le coronavirus : Singapour et la Corée du Sud, des exemples à suivre, L'Express, 18 March 2020. https://www.lexpress.fr/actualite/monde/asie/endiguer-le-coronavirus-singapour-et-la-coree-du-sud-des-exemples-a-suivre_2121024.html

Rombit (2020) Smart bracelet to prevent coronavirus infections on the workfloor, 17 April 2020. https://rombit.be/smart-bracelet-to-prevent-coronavirus-infections-in-the-workplace/

The ETUI is financially supported by the European Union.
The European Union is not responsible for any use made of the information contained in this publication.