Joint Statement on Digital Contact Tracing

by

Alessandra Pierucci, Chair of the Committee of Convention 108

and

Jean-Philippe Walter, Data Protection Commissioner

of the Council of Europe

Strasbourg, 28 April 2020

One month after our first Joint Declaration on the right to data protection in the context of the COVID-19 pandemic, countries and peoples around the world continue to relentlessly invest all efforts in preventing further propagation of the virus.

Since the start of the pandemic, governments and stakeholders involved in the fight against the virus, such as the scientific research community, have been relying on data analytics and digital technologies to address this novel threat.

Recalling that the data protection standards laid down by Convention 108 and its modernised version, Convention 108+, are fully compatible and reconcilable with other fundamental rights and relevant public interests, such as public health, it is crucial to ensure that the necessary data protection safeguards are implemented when adopting extraordinary measures to protect public health.

Regarding the use of mobile data and technology in the fight against COVID-19, specific measures are being deployed or otherwise proposed and include: use of mobile location data to evaluate movements of population or to enforce confinement measures, use of devices as digital proof of immunity, symptoms' detection, self-testing, or finally digital tracing of the contacts of an infected person.

All those innovative, or less innovative tools, rely on people possessing and carrying with them appropriate mobile devices. For example, people that do not possess a suitable mobile device will be excluded from such approaches. Furthermore, those tools which rely on the processing of personal data, have an impact on the privacy and data protection, and other fundamental rights and freedoms of individuals. It is crucial, therefore, to ensure that the measures and related data processing are necessary and proportionate in relation to the legitimate purpose pursued and that they reflect, at all stages, a fair balance between all interests concerned, and the rights and freedoms at stake, as the European Convention on Human Rights (Article 8) and Convention 108 + (Articles 5 and 11) prescribe.

Looking at contact tracing (and alerting) in particular, it should first and foremost be recalled that this monitoring process has always been used – manually - in epidemic monitoring to reduce the spread of infections; identifying the persons who may have come into contact with an infected person to alert them, where necessary, and allow them to get the necessary care and self-isolate to avoid further spread of the disease.

Mobile applications are now seen by many as a complementary response to the need to rapidly perform such contact monitoring. Indeed, mobile solutions that enable the automatic detection of contacts would save precious hours of work of public health staff tracing the chain of infection, could fill in important gaps that human memory would not be able to, and could do so with rapidity that matches the speed of the virus. Although technological tools can play an important role in addressing the current challenge, the first – essential – question we have to ask ourselves before systematic and uncritical adoption of technology (not having assessed their effectiveness and proportionality) is: are those "Apps" the solution? Considering the absence of evidence of their efficacy, are the promises worth the predictable societal and legal risks? Where governments decide to resort to this digital contact tracing in their management of the COVID-19 pandemic, what are the legal and technical safeguards that have to be in place to mitigate the risks at stake?

I. Effectiveness

As already spelt-out in the first joint declaration, "large-scale personal data processing can only be performed when, on the basis of scientific evidence, the potential public health benefits of such digital epidemic surveillance (e.g. contact tracking), including their accuracy, override the benefits of other alternative solutions which would be less intrusive."

The effectiveness of digital contact tracing depends on a multiplicity of factors, which are interrelated:

- a comprehensive national epidemiologic strategy articulating instrumental support to the public health system, manual contact tracing and a strong emphasis on widespread testing;

- the model chosen (technology used, architecture retained, definition of 'proximity' between the devices, both in terms of distance and duration, etc.); and

- widespread access to mobile devices and connection (which may also require specific technical functionalities such as "Bluetooth low energy"), while regretfully acknowledging that considerable segments of the population are unable to acquire or use them, in particular high-risk groups such as the elderly.

Where public authorities decide to use digital contact tracing, the following sections should guide the design and implementation of those systems[1], with the adoption of the corresponding appropriate legal framework to regulate the system.

[1] The "Guidelines on geolocation and other tracing tools in the context of the COVID-19 outbreak" adopted by the European Data Protection Board of the European Union on 21 April 2020 also provide important guidance on those questions. For more details: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

II. Trust and voluntariness

The acceptability of a digital contact tracing system clearly depends on the trust that such a system can inspire, and deliver. As public trust is essential for the broad adoption of the system, it is important to highlight that trust can be significantly strengthened through the integration of privacy enhancing features, and transparent information of the persons, regarding in particular the functioning of the system, its purpose and the data processed.

Achieving broad acceptability can thus be supported by implementing a trustworthy system, which is not imposed upon people but used on a voluntary basis instead. This also means that there should be no negative consequences imposed for not participating in the system.

Voluntariness does not mean that the processing of personal data will necessarily be based on consent as its legal basis. Convention 108+ allows the processing on grounds of public interest, including public health, provided for by law. Therefore, national laws, promoting a genuine voluntary recourse to such systems, would constitute an appropriate legal ground for this processing provided that the needed safeguards are put in place.

III. Impact assessment and privacy by design

Considering the likely impact of digital contact tracing systems on the rights and fundamental freedoms of individuals, their development should be based on a prior assessment of such a likely impact prior to their deployment.

Their design should be done in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms, to ensure notably that location data of individuals are not used, that no direct identification is possible, that re-identification is prevented.

IV. Purpose specification

The purpose of a COVID-19 digital contact tracing system is to identify persons potentially exposed to the virus and strictly excludes further processing of data for any unrelated purposes (e.g., commercial or law enforcement purposes).

Further processing of data for epidemiological research or statistical purposes would necessarily require an explicit consent.

V. Data: sensitivity, quality, minimisation

Health-related data are a special category of data which can only be processed where appropriate safeguards, which complement the other data protection requirements, are provided as enshrined in Article 6 of Convention 108+.

Considering the particular nature of location data, and the fact that proximity between persons can be obtained without locating them, digital contact tracing should be done on the basis of records of connections between devices rather than on the basis of location data (GPS generated data for instance).

As the implications may be serious (self-isolation, testing) for the individuals identified as potential contacts of someone infected, ensuring the quality and accuracy of data is crucial.

Data processed for digital contact tracing purposes should be reduced to the strictest minimum and any data that is not related or necessary should not be collected.

VI. Automated decision-making

Even in the current situation, individuals retain the right not to be subject to a decision significantly affecting them based solely on an automated processing of data without having their views taken into consideration. It is clear that implications such as self-isolation and testing can have such significant effects.

Users of the digital tracing system must therefore not have consequences imposed on them without a clear facility to challenge these consequences, particularly in light of the inaccuracies or misrepresentations possible in such systems.

VII. De-identification

Users of the digital tracing system must not be directly identified, and digital contact tracing systems should only use unique and pseudonymised identifiers, generated by and specific to the system. Those identifiers must be renewed regularly and must be cryptographically strong.

VIII. Security

Digital contact tracing systems have to include state-of-the-art encryption, communications security, secure development practices and user authentication to prevent from risks such as access, modification or disclosure of the data of the digital contact tracing system.

IX. Architecture

Digital contact tracing systems should be based on an architecture which relies as much as possible on the processing and storing of data on devices of the individual users.

Several models of centralised, partially centralised or decentralised architectures exist but none completely prevents from vulnerabilities and risks of re-identification.

X. Interoperability

Since the COVID-19 pandemic knows no frontiers, interoperability between systems should be ensured to enable the exchange of available information beyond national borders, provided that the necessary safeguards are ensured, including appropriate grounds for transferring data, robust security measures, and means to ensure accuracy of inbound and outbound data.

XI. Transparency

In light of the intrusiveness of digital contact tracing systems, full transparency through an open source development of the code is highly recommended, enabling anyone interested to audit (and possibly improve) the code.

Information provided to individuals should use clear and simple plain language.

Individuals have the right to obtain knowledge of the reasoning underlying data processing where results are applied to them, such as in the case of digital contact tracing. The general manner in which a particular digital tracing system works must be made fully public before and during operation.

XII. Temporariness

The data used for digital contact tracing should only be kept for the duration of the management of the COVID-19 pandemic and storage limitation periods should be defined in light of the epidemiological relevance of the data (such as the incubation time of the virus for instance).

At the term of that pre-defined period, all personal data should be deleted and technical measures enabling the automatic deactivation of the application and deletion of the data are to be supported.

XIII. Oversight and Audit

Digital contact tracing systems should be subject to independent and effective oversight and audits to ensure respect of the rights to privacy and data protection. Data protection authorities should be involved from the outset in the development of those systems, and use their powers of intervention and investigation to ensure that data protection requirements are enforced.

The COVID-19 pandemic creates unprecedented common challenges which require our greatest commitment, and caution. What is ahead of us belongs to political choices, to societal support and to our individual commitment. Despite the urgency, digital contact tracing raises new questions that cannot be neglected before deciding to implement such population wide measures. Beyond privacy and data protection considerations, digital contact tracing approaches raise questions of inequality and discrimination that also have to be considered.

Alessandra Pierucci and Jean-Philippe Walter