COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Cres
Droit, religion, entreprise et société
University of Strasbourg

AI&Law Breakfasts

5th edition: Myths and realities of tracking applications

Summary of interventions

Guests: Michael Veale, Lecturer in Digital Rights and Regulation, University College London, **Dino Pesdreschi,** Professor of Computer Science, University of Pisa and **Adrien Basdevant,** Lawyer, Member of the Paris Bar

Covid-19: Myths and realities of tracking applications
Michael Veale
Lecturer in Digital Rights and Regulation, University College London
Dino Pedreschi
Professor of Computer Science, University of Pisa
Adrien Basdevant
Lawyer, Member of the Paris Bar
online on 16.04.2020
Web: http://www.coe.int/ai
Twitter: @coe4ai
Facebook: coe4ai

The three speakers presented their analyses on mobile phone applications designed (or in the process of being designed) in many countries in order to support *contact tracing* policies. Decentralised technical modalities such as the DP-3T protocol make it possible today to envisage the deployment of such applications while respecting the privacy of individuals. Consequently, their use could usefully support the work of epidemiologists and health personnel in tracing the chains of propagation. Nevertheless, a number of issues remain to be addressed before their deployment, such as the trivialisation of the use of these technologies, which could be used for other purposes and in other contexts, as well as their reliability and robustness. Are we moving into a new age of surveillance?

Michael Veale

Lecturer in Digital Rights and Regulation, University College London

His research sits at the intersections of emerging digital technologies, Internet and data law, technology policy and human-––computer interaction. He pushes a decentralised approach to Covid-19 contact tracing.

Michael Veale presented the DP-3T anonymised registration protocol. This protocol is decentralised by nature with functions presented as useful for epidemiologists. The tool would allow them to process mass of data while limiting the disadvantages of data collected in one place (centralised) - which could be misused or cross-referenced with other files.

According to Michael Veale, geographic location would not necessarily be a relevant indication for epidemiologists. In addition, there would be many technical constraints related to geolocation (such as faster battery discharge due to GPS tracking). The idea therefore arose to use the Bluetooth Light Energy (BLE) functionality, theoretically present in most phones since 2010, and which makes it possible to estimate a distance based on the strength of the signal exchanged between 2 phones.

Michael Veale gave an overview of how a *contact tracing* or *proximity tracing* system works. If someone reports (voluntarily) being sick in the application, the system recomposes a list of people with whom s/he may have been in contact at a distance of 2 or 3 metres over the last few days. By means of computer processing, these people then receive a completely anonymous alert with options for action.

In practice, there are two main ways to achieve such a system:

1. By generating a random number identifying the mobile phone, then sending it to a central server - the difficulty is that there can be possible misuse of this database;

2. Your phone listens and sends its random, anonymous number directly to other phones that have been in contact during a defined period of time. If you declare yourself sick, you can send your contact history to a central server. The server only retrieves random numbers, which do not directly identify persons. Then, on a regular frequency (every day for example), all users download the last anonymised list and it is their phone that checks if a correspondence occurs with the random numbers it has previously generated. With this system, nobody has the complete puzzle.

This protocol has been widely opened to developers and cryptographers who have been able to make proposals, criticisms and suggest improvements. The Google - Apple partnership announced to launch a protocol quite similar to the DP-3T. But each State is naturally free to use the protocol that it wants, and nothing obliges to use the one proposed by Google and

Apple. It should be noted that the Bluetooth functionalities of Apple's phones (iPhone) are less easily usable by third party applications and in Singapore, for example, users of this brand have been obliged to leave their phones open and unlocked (which can create a lot of difficulty in case of theft etc). Nevertheless, Apple seems to want to make access to these Bluetooth functionalities more flexible for this type of anonymous tracking application (such as DP-3T).

These protocols cannot, however, ensure that member States will not make more coercive use of them. No code will be able to protect against this and we need the law, respect for human rights. We must be able to ensure that the risk calculation system does not infringe fundamental rights.

Dino Pedreschi

Professor of Computer Science, University of Pisa

He is a pioneering scientist in mobility data mining, social network mining and privacy-preserving data mining. He contributes with Marco Nanni, Virginia Dignum and other searchers to a manifesto called ‘Give more data, awareness and control to individual citizens, and they will help COVID-19 containment”.

Dino Pedreschi believes, based on his experience in the Italian government's task force, that the use of data and models can help in the fight against the epidemic, especially after containment.

Work on computer tools is being done very closely with epidemiologists and health workers to build an effective monitoring system. Two main elements are necessary:

1. To be able to test people to find out if they have been in contact with the virus, so that they can be quickly isolated and asked who their recent contacts have been in order to reconstruct the chain of possible contamination. This is *contact tracing* in practice: an army of "firemen" who can identify new possible outbreaks and contain them as quickly as possible.

2. We must be able to do the same thing at the level of the entire community when many cases are clustered geographically.

But even before discussing applications and digital, the basic question is how citizens can help "firemen" do their jobs and protect the public good of public health. Can we participate actively in this fight rather than passively waiting to be tested and follow the procedure if we are ill? Confinement has already been an example of this, where we restrict our freedoms to help in this fight. Now it is a matter of finding collective active ways to deal with this problem and, of course, when freedoms are restricted, we need to know the justification and duration. There are two possible approaches: either to force people to take part in this digital surveillance, which does not seem compatible with democratic requirements, or simply to encourage them to do so, which seems to be the case with initiatives in Europe.

The DP-3T protocol presented by Michael Veale fully supports the work of these "firemen" by allowing them to trace more contacts. It's actually a way to extend the memory of a person who has tested positive to know what his or her contacts have been over the last few days. Mobile phones can be used to assist *contact tracing,* in a completely anonymous and decentralised way. This somehow automates the work of an epidemiologist, since people will receive an alert informing them that they have been in contact with someone who has been infected with the virus and that they could voluntarily contact the authorities to be tested. We need to think about these totally decentralised approaches, with data shared with no one, and based on the voluntary approach of infected persons to contribute to public health. Under these conditions, this approach does not seem problematic to Dino Pedreschi. He recalls that, in order to contribute to this tracing, there is no need to constantly check the exact trajectory of the persons: what is important is that - if you have been tested positively - you are able, thanks to these applications, to tell others, voluntarily and very precisely, where you have spent most time, during the last few days.

Unlike Michael Veale, Dino Pedreschi believes that epidemiologists are interested in data on localisation, because geolocalisation of new positive cases is interesting for identifying new clusters of cases and possible new outbreaks. This then requires other treatment methods other than *contact tracing*.

Dino Pedreschi acknowledges that everything depends on how the system will be used at a national level. What seems important to him in the proposed applications is that information is only disclosed on a voluntary basis and in a completely privacy-friendly manner, and whether it is contact tracing or the location of a person, only when the person has been identified as positive for the virus.

Dino Pedreschi reminds us that in order to achieve this digital *contact tracing*, different ways have been developed, including the DP-3T protocol. Yet, what it is really important to keep in mind, besides the features of each specific application, is that digital technologies are only one of the elements of the response to the problem, a response which needs to be global and requires a very strong investment from people. The work of epidemiologists, of "firemen" can be supported by digital technologies, but we are not going to win this battle with an "app". This must be clear, there is no magic in this. If there is a sufficient mass of citizens participating in this mobilisation, then we can hope to significantly reduce the epidemic. This is typical of other phenomena, such as car traffic, when you reach a certain threshold, you can really improve things very quickly and this is also true for epidemics. If we propose "games" in which people trust to improve the public good, we will not engage everyone. But even if 30, 40 or 50% participate, it could really help contain the epidemic in the post-containment phase and allow us to gradually return to our activities and freedoms.

Furthermore, Dino Pedreschi mentions the publication of a manifesto on data recording. For several years now, many researchers have been supporting the idea of restoring power to people to manage their data, with exclusive control by them and open to no one (even the police). This is a tool that could be implemented on a voluntary basis, which could be applied to any activity that an individual would choose, with very strong guarantees for privacy and security. Such a data storage tool makes it possible to voluntarily share anonymised information for the common good and could help to better manage problems such as mobility or traffic jams. And if we already had this kind of tool, which could have been done in a completely secure way with respect for privacy, it could have been useful in dealing with a crisis such as this epidemic.

Adrien Basdevant

Lawyer, Member of the Paris Bar

He focuses on data protection, cybercriminality and emerging technologies. He defends civil liberties in the information society, and advises numerous startups. Author of “L’Empire des données” and lecturer at ESSEC-Centrale Supélec, he is working at the intersection of law, tech and policy.

Adrien Basdevant wonders if such a state of health emergency has ever been known in our history. The French philosopher Michel Foucault explained that in Western Europe we have used two main ways to deal with epidemics and control populations: the first model was exclusion for people with leprosy and the second was inclusion and containment for the plague. According to Foucault, the transition from one model to the other was one of the most striking events of the 18th century.

And it was precisely in the 18th century that statistics first appeared. Today we have *big data* (either advanced statistics or metadata analysis) and one wonders whether we are not seeing the emergence of a third model of individual control. For leprosy, a model of exclusion has been applied which could be called a model of marginalisation: the practice was then, in a very harsh way, to reject patients beyond the city walls. In this model, patients were very simply left to die outside the city, to make sure that others would not be infected. In the other case, for the control of the plague, the population is no longer rejected but confined within the city walls. This was called quarantine and there were inspectors who passed and stopped in front of each house to call out the names of the occupants and check their health. People were thus sorted into those who were sick and those who were not, and this made it possible to rigorously quantify the different populations (sick and healthy) and to try to treat them. This is how we moved from punishment (ban) to discipline.

Foucault demonstrated how statistics have revolutionised the control of pandemics and persons. Statistics have made it possible to measure mass phenomena and allowed us to move from brutal policies of exclusion to what has been called political arithmetic. And statistics are to be understood as an objective instrument of state control, making it possible to distinguish between "normal" and "abnormal" behaviour. This is how Foucault describes how individuals and populations have become the object of disciplinary measures and how corrective mechanisms are then applied, which Foucault called biopower, which literally means exercising power over bodies and which is of course a power of normalisation. One might wonder what Foucault would think today as he moved from statistics to *big data*.

Extending his reasoning, one may wonder whether the 21st century is not becoming a 3rd age of personal control. Not that of exclusion, not that of inclusion by confinement or quarantine, but that of inclusion by tracing. This amounts to allowing a certain capacity to come and go in return for real-time surveillance. When you are confined as with the plague, you are only limited in your freedom of movement. But when you're no longer confined and you're using an application, you're in a different model of inclusion where you're no longer limited in your movements but potentially in your digital freedoms. The model of inclusion through tracking raises new challenges and issues. It seems harmless because it is based on voluntary submission, but it can become binding and compulsory as in South Korea, China or Israel, by making it part of ordinary law. This shift reveals new capacities for state surveillance of individuals, with a kind of social peer tracing.

More substantially, Adrien Basdevant believes that this may also create new cases of discrimination. Obviously, whether it is the plague or Covid-19, there is discrimination, but it seems less tangible and less visible. A concrete example of social stigmatisation is the transformation, as a result of *contact tracing* or *proximity tracing*, of a simple measurement into a diagnosis. The question we should ask ourselves is how precise this measurement is: how are we going to be able to avoid, for example, false positives? If you imagine a cashier in a shop behind a Plexiglas window, he or she will have a mask and gloves on, this person will meet a lot of customers during his or her working day. Some of these customers will certainly be contagious, but that doesn't mean that this cashier will also be contaminated. And that's the whole problem with *proximity tracing,* which is how this application will define a proximity that is close enough to be contaminated - which today cannot be defined precisely enough. The criteria of this proximity are generally defined by the contact time, the distance (2 or 3 meters in general) and the question is, for all these criteria, that of their precision and reliability.

The reliability and effectiveness of these measurements is really important: in other words, if the conditions under which the system can make a decision are not precisely defined, there will necessarily be persons subjected to forced quarantine when they should not, and this may amplify existing inequalities. The trivialisation of the use of such technologies may also lead to the acceptance in the short or medium term of an application of this type in another context, such as for the maintenance of public order or the control of employees. This type of application should remain optional for any citizen, user or customer, and this type of device should not be put in place in order to get a kind of "green light" before entering a shop, benefiting from a service or going to work.

In conclusion, Adrien Basdevant has two points to consider.

According to him, we should first develop multi-factor impact studies, in order to implement responsible data sharing in times of crisis. Two legal frameworks already exist to help with this: Convention 108 from the Council of Europe and the RGPD. If we take the data protection impact assessment studies as a basis, we should be able to improve them and extend them to new rights. As an example, this type of study should show that it should be possible to voluntarily stop tracing: if you are planning to do so in two months' time, with an application installed on your mobile phone, you should be able to avoid giving out information because you are in a particular context (personal, political, religious). Adrien Basdevant points out that we should also avoid confusing privacy and data protection: we would often talk about PIA (*privacy impact assessment)* and not DPIA (*data protection impact assessment*). Adrien Basdevant reminds us that these are two distinct values. The fact that we refer to privacy shows that we sometimes forget the other social values at stake, such as the existence of due process, fairness or non-discrimination. It should therefore be suggested that if these data protection studies are strengthened, other dimensions such as non-discrimination or the digital divide should be integrated to ensure that already marginalised populations are not left behind.

The second element of reflection for Adrien Basdevant would be to consider legal standards to frame the anonymisation of data. We know that personal data is defined as information that identifies, directly or indirectly, a natural person. Anonymisation, on the other hand, relates to information that does not allow reidentification, without any possibility of reversibility. Case studies and scientific publications have shown how difficult it is to create a truly anonymous dataset. The problem here is that we have no international or regional standards on this subject. The only document is the G29 Opinion No. 5 published in 2014, which is no longer completely up to date with the latest state of the art. The priority today could be to define the acceptable threshold for a data item to be considered anonymous and we should have a debate, if an application such as for those to combat coronavirus contamination, on whether or not re-identification is - or is not - possible given the means that can reasonably be used. This may be the way to preserve innovation while protecting individual freedoms.

Go further

Links proposed by Michael Veale:

- The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates
- DP-3T protocol documentation

Link proposed by Dino Pedreschi:

- Give more data, awareness and control to individual citizens, and they will help COVID-19 containment

Link proposed by Adrien Basdevant:

- Covid-19: a new era of individual control?