# Anonymous tracing, a dangerous oxymoron

## A risk analysis for non-specialists

An article by

**Xavier Bonnetain**, University of Waterloo, Canada ; **Anne Canteaut**, Inria ; **Véronique Cortier**, CNRS, Loria ; **Pierrick Gaudry**, CNRS, Loria ; **Lucca Hirschi**, Inria ; **Steve Kremer**, Inria ; **Stéphanie Lacour**, Université Paris-Saclay, CNRS ; **Matthieu Lequesne**, Sorbonne Université et Inria ; **Gaëtan Leurent**, Inria ; **Léo Perrin**, Inria ; **André Schrottenloher**, Inria ; **Emmanuel Thomé**, Inria ; **Serge Vaudenay**, EPFL, Suisse ; **Christophe Vuillot**, Inria.

Contact : contact@risques-tracage.fr Web: https://risques-tracage.fr/

*Translated from the French by Tom Lancaster (tom.lancaster@durham.ac.uk).*

In an attempt to arrest the progress of the COVID-19 epidemic, France plans to put in place a system intended to trace patients using a mobile app. The developers of this type of app intend to ensure that they are respectful of privacy. However, this notion remains vague. We hope, therefore, to contribute to the public debate by clarifying what a tracking app could and could not guarantee, with the intention that people can form an opinion on whether its deployment is advisable.

The usefulness of this application lies in its capacity to detect contacts at risk, and to use this information in a relevant manner with other measures to fight the epidemic, such as screening or quarantine. Not having expertise in epidemiology, we are mindful of not judging the impact of the tracking app on the spread of the disease. However, this evaluation would seem indispensable to balance the possible benefits and risks.

Our expertise as specialists in cryptography, security or technology law lies, in particular, in our ability to anticipate the multiple abuses and misappropriations, and other malicious behavior, that could emerge. At present, a lively debate is ongoing on the proposed applications between specialists in the field of security, often pitting so-called "centralised" applications against "decentralised" ones. Regardless of these technical considerations, we intend to alert people to the intrinsic dangers of a tracking application. Using different scenarios such as the one below, we elucidate the possible abuses of such a technology, regardless of the details of its implementation.

**Scenario.** *The KROOKS company intends to recruit a temporary employee. They want to make sure that the candidate does not fall sick between the job interview and signing the contract. They therefore use a dedicated phone that is switched on only during the interview, and which will receive an alert if the candidate later tests positive for the disease.*

**Summary**

| | |
|---|---|
| – There is no patient-name database. | ☑ **TRUE** |
| – Data is anonymous | ⊘ **FALSE** |
| – It is impossible to find out who has contaminated whom | ⊘ **FALSE** |
| – It is impossible to know whether a specific person is sick or not | ⊘ **FALSE** |
| – It is impossible to trigger a false alarm | ⊘ **FALSE** |
| – Using Bluetooth is not a security issue | ⊘ **FALSE** |
| – The system makes large-scale snooping impossible | ⊘ **FALSE** |

## Introduction

The world faces the COVID-19 epidemic. Many countries, including France, plan to set up a system for tracking patients' contacts using a mobile app. The guiding principle is that if someone has tested positive for the virus it will be possible, by using the application, to alert all of the people with whom they have recently had contact and, in doing so, encourage them to self quarantine, to consult a doctor, or to be tested. Since the beginning of the epidemic, researchers in computer security have invested effort in the design of such systems; others like R. Anderson [1], S. Landau [2], B. Schneier [3] and S. Vaudenay [4], have spoken of the dangers of such a system, or have spoken out against its implementation. Given the potential risks to privacy, the use of such an application has initiated a debate.

In the first place, these apps only make sense if they really allow the detection of contacts at risk. This assumes that tracking applications can accurately assess the distance between people (perhaps to an accuracy of one meter), whatever the environment or position of the phone. In practice, it will be necessary to make a compromise, but there will likely be both undetected contacts (including cases of transmission via surfaces) and false alarms (such as a detection made through a wall). The plan also presupposes a mass adoption of these solutions by the population, which generally require a smartphone and often Bluetooth.

Contrary to current practice[1], these technologies alert people who have been in contact with a patient in a systematic and undifferentiated manner, such that both the patient and professionals are deprived of the ability to determine who it is necessary to alert. We could question, for example, the need to advise all contacts to travel for a test, since for the elderly or those with pre-existing illnesses, this would represent an additional risk. These aspects are often addressed very little in the public-facing documentation on the proposed applications. We shall therefore not discuss the effectiveness of the tracking applications here, but rather their safety, even if it seems essential to us to assess their effectiveness and compare it with that of the existing procedures, or the detection of clusters by epidemiologists.

The question of the risks to public freedom has already been raised, notably by Quadrature du Net [7]. Our contribution will be limited to the study of several scenarios, in order to highlight the creep that such application would make possible. Even if some of these security holes could be partly avoided by significant modifications to the proposed protocols, most of the scenarios we envisage are inherent in the features of these apps.

We begin by presenting the general operation of this type of app. The scenarios are discussed starting from Section 4.

1. The existing procedure is based on disease-reporting mechanisms and the authorities making an investigation aimed at tracing an infected person's at-risk contacts. The public authorities then alert these contacts and advise them. By attempting to mimic these existing procedures with a technical solution, we also neglect that fact that the implementation of the rule of law always gives rise to many provisions [5, 6].

# 1 Device operation

Our analysis focuses on recent proposals for a tracking system using Bluetooth. These systems have been proposed as a more satisfactory solution with respect to privacy than those based on the precise geolocation of members of the population, as was carried out in China, and about which most European countries, as well as the European Commission [2], have shown themselves reluctant to consider. Several alternative tracking systems [3] have been proposed in the last few weeks by IT security specialists, researchers and by industry. In particular focus in our study are (and this is a non-exhaustive list): the DP3T [4] protocol (various variants), its variation by the Apple/Google [5] alliance, the PACTEst [6] protocol, the PACT-Ouest [7] protocol, the TCN [8], protocol, the ROBERT [9] protocol. **The synopses of most of these systems promise to "respect the privacy of users". But it is important to elucidate what this slogan means (and does not mean).**

We take this opportunity to recall a fundamental principle in computer security: it is essential that the description and the code of a system are published and evaluated in order to instill confidence in it.

## 1.1 General principle

Various published variants of "privacy-respecting" tracking systems all follow a pattern relatively close to that illustrated in the strip drawn on page 4. The mobile phone of each user frequently (e.g. every 5 minutes) generates a random code (a series of letters and numbers), that we shall call a pseudonym. Whenever two phones are in contact nearby, they exchange their current pseudonyms via Bluetooth [10], and note the date and time of the exchange. This information is stored in the telephone of each user for two weeks. When a user (let's call her Alice) is tested positive, the app alerts all the people with whom it has exchanged pseudonyms in the previous 14 days, such as the user Bob, for example. Bob then receives a notification (with recommendations based on the time spent in contact with the patient). The procedure allowing the application to use pseudonyms to prevent contact depends on certain protocols and will be detailed in the next section.

## 1.2 Who certifies that Alice is sick?

When Alice gets sick, she has to trigger the app so that people with whom she has been in contact will be notified. But who certifies that Alice is sick and that the

2. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670, consulté le 18 avril 2020.

3. These systems do not allow not to identify "clusters" since they do not use any geolocation information.

4. DP3T = *Decentralised Privacy-Preserving Proximity Tracing* https://github.com/DP-3T/documents/ consulted 18 April 2020.

5. https://www.apple.com/covid19/contacttracing/ consulted 18 April 2020.

6. PACT = *Private Automated Contact Tracing*, https://pact.mit.edu/ consulted 18 April 2020.

7. https://covidsafe.cs.washington.edu/ consulted 20 Aprril 2020.

8. https://tcn-coalition.org/ consulted 20 April 2020.

9. ROBERT = ROBust and privacy-presERving proximity Tracing, https://github.com/ROBERT-proximity-tracing/documents/ consulted 18 April 2020.

10. Note that Bluetooth is not designed to test physical proximity and, in fact, will assume that two people on different sides of a wall have been "in contact". However, its use avoids the use of geolocation methods that reveal the precise position of people's movements.


FIG. 1 – *The operation of the app in the decentralized model (used by D3PT and Apple/Google). Centralized protocols such as ROBERT don't follow the same procedure to warn Bob when Alice gets sick. [Figure from a drawing by Nicky Case (ncase.me).]*

information should be transmitted? There are two possibilities:

1. Alice self-diagnoses and triggers the report herself.
2. Alice's disease must be confirmed by a test or a medical professional for the information to be disseminated (for example, giving Alice a single-use code that will trigger the alert).

We shall only consider the second possibility, which seems to be the option chosen by the protocols proposed in Europe[11]. Indeed, if people can declare themselves sick without the certification of a medical authority, any malicious user can make false declarations of illness, as in the following scenario. The multiplication of such false reports will quickly render the system inoperative.

**Scenario 1** (False declaration)**.** *Soccer player Gronaldo is to play in a forthcoming Champions League match. To prevent him from playing, it is sufficient for an opponent to leave his phone next to Gronaldo's without Gronaldo's knowledge, then for the opponent to declare himself sick. Gronaldo will receive an alert because he has supposedly been in contact with an infected person, and will have to stay away from the football pitch for 14 days.*

## 2 There is no patient name database

We have not yet explained how it was possible to warn Bob that he has been contact with a sick person. A simple idea (risky in terms confidentiality of medical data) would consist of establishing a list of sick persons. This idea is disregarded by "privacy-respecting" apps, which prefer two alternative solutions, corresponding to two different models of data dissemination.

1. **The "decentralised" model.** When diagnosed, Alice sends everyone the list of pseudonyms that she has transmitted in recent days. Technically this can be done as a peer-to-peer operation, or through an intermediary, such as a health agency, exemplified by a hospital[12] in the comic strip. Bob can query this database to find out if it features any of the aliases that he has recently received. If there is a match, the app sends Bob an alert. DP3T, PACT and Apple/Google protocols follow this pattern.
2. **The "centralised" model.** When diagnosed, Alice sends the central authority the list of pseudonyms that were recently registered. This list of contacts at risk is not published and is only known to the central authority. In this model, Bob, like each user, contacts the central authority daily, and provides them with the list of pseudonyms that he has transmitted[13] to find out if any of them is in the database of at-risk contacts. If necessary, he receives a notification.

Both of these models have advantages and disadvantages. The centralised model requires trusting a central authority. For example, the authority can use the list of contacts received by "new" patients, and detect those individuals who have previously been reported as having been exposed to the virus, noting that they have previously disregarded their quarantine guidelines. The decentralised model does not *a priori*

11. It seems essential, for the system to work, that these reports rely on tests that are reliable.
12. This is the choice made in DP3T, PACT and Apple/Google protocols.
13. In the particular case of ROBERT, the central authority calculates all the Bob's pseudonyms , although it doesn't know his identity a priori.

pose this problem, but does open the door to other attacks. These two models will be studied later. Their differences are significant, although most of the scenarios we discuss will work regardless of the model.

## 3 Data is not anonymous

Decentralised tracking protocols do not require the creation of a register of COVID-19 patients, as required for certain reportable diseases defined by law. Centralised models possess a database of people at risk of contracting the disease after they have been in contact with a case of the illness. In both models, these files are pseudonymised, which means that the patients are not identified by their name or social-security number, but by a code or a number that is independent of their real identity. In the proposed systems, the file of COVID-19 patients is pseudonymised with cryptographic mechanisms[14] as is the case, for example, for the register of declarations of HIV-AIDS. However, this number could be de-anonymised by combining it with other information in the database (the identifiers of people who have been in contact), or outside of the database (for example, collected with a Bluetooth antenna), or by IP address. **It is not, therefore, an anonymous database** such as defined, for example, by the GDPR.

> “ *Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.* ”
>
> — General Regulation on Data Protection (GDPR)

This database therefore contains personal data within the definitions of the GDPR and the French law[15]. It also contains data classed as sensitive (i.e. medical data), access to which confers particular requirements, in particular by limiting the possibility of processing it[16].

**Anonymous and Pseudonymous?**

- Mr. Bloggs is sick — ⊘ **NOMINATIVE**
- The pseudonym `439Hxs` is sick — ⊘ **PSEUDONYMOUS**
- There are 50 437 cases — ☑ **ANONYMOUS**

## 4 How do you find out who infected you?

Although patients' pseudonyms do not disclose their identities, users can easily infer information about other users as soon as they learn that a person they have met in the past two weeks has fallen ill.

14. For example, the DP3T and Apple/Google protocols use HMAC-SHA256 which is considered safe at present.

15. In the sense that this data makes it possible, even indirectly, to identify the persons concerned.

16. Article 6 of Law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms last amended in 2019 and Article 9 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, relating to the protection of individuals with regard to processing personal data and the free movement of such data, and repealing the directive 95/46/EC (general regulations on data protection).

**Scenario 2** (The sole suspect)**.** *Mr. Smith who, to avoid contamination, never leaves his home apart from to do his shopping at the neighborhood grocery shop, receives a notification from his telephone. It follows*[17] *that only the grocer can be responsible.*

**Scenario 3** (Information crossing)**.** *Mrs. Jones, who encounters a lot of people during the day, receives a notification. She just has to chat for a few moments with her next-door neighbor and an office colleague, to find out that the patient is not a professional colleague, but that they live in the building. Thanks to these clues, she strongly suspects (perhaps wrongly) that Mr. Attrisk on the 3rd floor, who is a paramedic, has contaminated all of its neighbours. She hastens to warn the rest of the inhabitants of the building via social networks.*

These believable scenarios are completely independent of the details of the app. They do not require any particular computer skills. They illustrate the limitations inherent in this type of system. Even if it is not *a priori* possible for the central authority to circumvent the pseudonymisation of users, it is not difficult for a user to do so.

These tracking technologies have the feature of systematically and indiscriminately warning all of the people encountered by a patient, and cannot instead be a voluntary and considered notification of close contacts of the sick person. In decentralised models, it is the population in its entirety that receives the health data collected by the system, which is radically different from all existing systems.

To the extent that tracking would act as a whistleblowing system on a large scale, the information that it brings would cause suspicion, would transform possible contamination into moral fault[18] and exacerbate the stigmatisation of people at risk in an already sensitive context. Such effects have already been reported in Korea, for example[19], causing witch hunts. This risk of stigmatisation has been regarded as being of concern since the register of people living with HIV was created twenty years ago, and this concern seems even more legitimate in the age of social networks.

**Scenario 4** (Are my neighbours sick?)**.** *Mr. Hipokondriac would like to know if his neighbours are sick. He finds his old telephone in a cupboard, installs the TraceVIRUS app, and leaves it in his mailbox at the bottom of his building. All of the neighbours pass by each time they return home, and the phone will receive a notification if one of them is sick.*

17. We note that Mr. Smith might be wrong: his notification could be due to another neighbor, who is sick, and whose smartphone was detected by Mr. Smith's through the wall.

18. Tracing is an individualising management solution to the complex problem of of containment. This interpretation can be based on the work of researchers in the social sciences, for example [8], which show that the evolution of our health system over recent decades has led to an enhancement of the figure of the rational and informed individual, responsible and capable of making informed choices, based on government information and economic incentives. The response envisaged through the use of this type of app goes in the same direction

19. In South Korea, residents can receive alerts that someone living the same neighborhood has tested positive for the virus. These alerts give their sex, age and the list of their recent trips. Although *a priori* anonymous, this information could lead to identifications by the public, followed by online emigration campaigns (one is accused of having potentially spread the virus). https://www.bbc.com/news/world-asia-51733145

## 5 How do you know if a specific person is sick? Spying within everyone's reach

In essence, all tracking systems that notify patient contacts can be used to find out if a particular person becomes ill. To have reliable information about a specific person, we just use a dedicated phone on which we install the app[20], and put the phone in contact with only this person. The two phones will record the contact, and if the target is tested positive our phone will receive an alert.

**Scenario 5** (The job interview)**.** *The KROOKS company intends to recruit a temporary employee. They want to make sure that the candidate does not fall sick between the job interview and signing the contract. They therefore use a dedicated phone that is switched on only during the interview, and which will receive an alert if the candidate later tests positive for the disease. (See Fig. 2.)*

Many similar scenarios are possible (e.g. a banker who is reluctant to make a loan to a client), all of these scenarios are very simple to put in place.

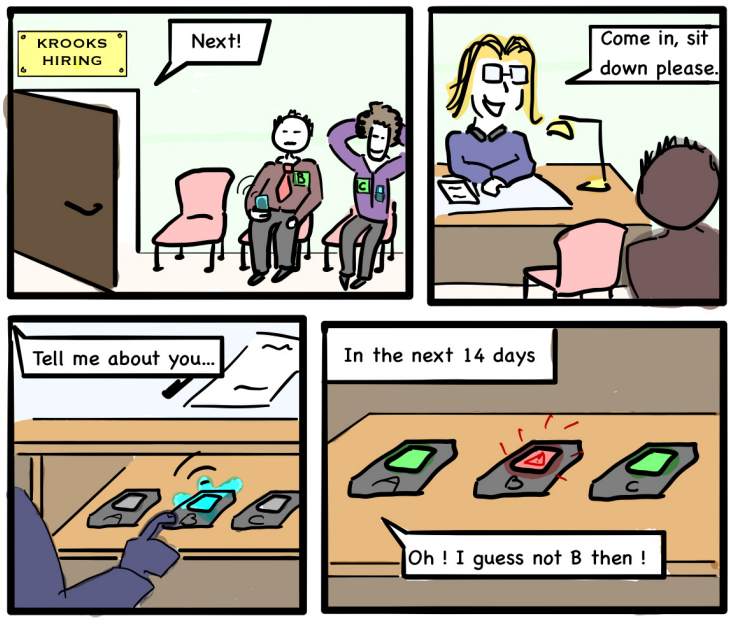


FIG. 2 – *Possible hijacking of the app during a job interview.*

**Scenario 6** (The paparazzi)**.** *Mr. Paparazzo seeks private information from Mrs. Star. He bribes Ms. Rimelle, the makeup artist who works on the set of Star's latest film so that Rimelle turns on a dedicated phone and places it nearby Mrs. Star's. Mr. Paparazzo then picks up the phone. He will receive a notification if Ms. Star is infected with the virus.*

Depending on the technical details of the protocol, it might be possible to create false identities in the app to trace a large number of people without having to buy a

20. Simple techniques also allow the same application to be installed multiple times on the same phone, that further facilitates such an approach.

phone for each target. One can also receive Bluetooth messages over a long distance (more than a kilometer [9]) with a dedicated antenna. In the decentralised model, we therefore capture the pseudonym of the target, and can check if they are among those identified as sick within two weeks. The previous attack scenarios are possible for all tracking protocols envisaged, but simpler to implement in the decentralised model.

# 6 How to trigger a false alarm, and make it look like someone is at risk of being sick

**Scenario 7** (The anti-system activist)**.** *Mr. Spart, who has symptoms of COVID-19, is an anti-system activist. To protest against the implementation of the TraceVIRUS app, he ties his phone to his dog, and lets him run around in the park all day. The next day he goes to see the doctor and is tested positive and all dog walkers receive a notification.*

**Scenario 8** (Foreign interference)**.** *The Terrifying submarine must sail in a few days, but John Bond is a foreign agent who wants to prevent its departure. He recruits Sniffles Galore who displays symptoms, and asks her to go around water-front bars. Sniffles Galore will then be tested, and five sailors will receive an app notification. The Terrifying is then forced to stay in the dock.*

The same scenario can be used to target specific people (an opponent in a sports competition, a competitor for a job interview, a key person during a negotiation etc.) or collectively on a large scale to make a whole system inoperative. The possibility of triggering false alarms could also be exploited in scenarios in which a user pretends to have met a patient in order to be tested first, to benefit from sick leave, or to escape an occasion that they dread, as in the following scenario.

**Scenario 9** (The pupil Bart Symptomson)**.** *The pupil Bart Symptomson has a test next week, but he did not revise. Thanks to a classified ad, he finds Mr. Sneeze who has symptoms and agrees to lend Bart his phone. Bart passes Mr. Sneeze's phone throughout the class, then hangs around the staffroom. Bart then returns it to Mr. Sneeze, who goes to see a doctor. The doctor notes that Mr. Sneeze is ill with COVID and reports him via the app. This triggers an alert for the whole class and for all teachers, causing the school to be closed!*

# 7 Turning on Bluetooth poses security concerns

The simple act of activating Bluetooth on your phone poses security and privacy problems, which is why it is generally recommended to deactivate it as often as possible.

Its use can open security holes that would exploit bugs in the phone's Bluetooth system. Specifically, the Blueborne attack [10] published in 2017 makes it possible to take control of many electronic items (computers, telephones, etc.) by exploiting this type of bug. If some phones have not been updated since 2017, then activating Bluetooth could be very dangerous!

The Bluetooth signal can also be used to trace users. We have all seen how easy it is to identify neighbours' Bluetooth devices or those of travellers on a train. Generalising its use opens up many possibilities.

**Scenario 10** (Burglary)**.** *Ms. Beagle wants to rob Uncle Duck's house. Before entering, she uses an antenna to detect Bluetooth signals. She knows that Uncle Duck is using TraceVIRUS, and if there is no signal, the house is empty.*

**Scenario 11** (Mall)**.** *The Snitch Avenue shopping center wants to protect its customers, and reject those who are not using the TraceVIRUS app. Since the app regularly broadcasts messages, the security guard at the entrance needs only to use a Bluetooth antenna to detect which customers use the application and which do not.*

Several department-store chains already use Bluetooth tracking to follow their customers in the store and better target advertising [11]. If the use of Bluetooth is generalized, one can imagine many ways to use it for many other kinds of tracking.

## 8 Towards large-scale snooping?

Even if the envisaged app will not itself track the sick, it is possible to use the signals exchanged by the app to create a large-scale register of the sick. The difficulty of creating such a database varies with the technical details of the protocol used. It is particularly easy with a decentralised system, because the list of pseudonyms of patients is public, and it suffices to re-identify them. With a centralised system, you have to be able to create a false identity or use a new telephone, then get in contact with the person you seek to trace. In any case, it will be difficult to define a protocol that completely avoids this type of attack.

**By users.** Tracing can be done by the users themselves, with the goal of better protection. The information exchanged for tracking is at the local scale. But if users join forces, they can recreate global information, as in road radar-detection apps. For example, we cannot prevent the appearance of an "improved" app (let's call it GeoTraceVIRUS) that would record the places where patients are, in addition to trace direct contacts with patients.

In a decentralised system, it suffices for GeoTraceVIRUS to record the GPS coordinates at the same time as the Bluetooth messages it receives. When a pseudonym is declared sick, GeoTraceVIRUS allows to know exactly where the patient was when he received the contact, and shares this information with other users. In a centralised system, GeoTraceVIRUS can record the movements of users, and crosscheck when certain users receive a TraceVIRUS notification. With enough GeoTraceVIRUS users, this at least makes it possible to locate the district in which the patients live.

**Scenario 12** (The GeoTraceVIRUS application)**.** *Shortly after installing the app TraceVIRUS, Mrs. Jones hears about the GeoTraceVIRUS app that uses TraceVIRUS information to locate patients. Mrs. Jones thus learns that a patient went to LowPrice supermarket last Saturday. Out of (perhaps unfounded) fear of catching the virus, she will not go shopping at LowPrice this week.*

Another "improved" application that users might be tempted to install would offer to boost the Bluetooth signal, so that one can be warned in case of less close contact with patients. Some of these alternative applications could be malicious, and could grab users' private data. Regardless of the quality of the official application, the Bluetooth signals on which it is based on can be reused by other apps in a proliferation that seems difficult to manage.

**By data analytics companies.** Following the Cambridge Analytica scandal [12], we know that some companies are not hesitant to collect data in a illegal manner for financial benefit. Insurance companies or unscrupulous employers might be interested in a list of COVID-19 patients, if, for example, having contracted the disease increases the risk of subsequent illness. Even if the state does not have such a list, the use of a tracking application makes possible the creation of such a database by private agencies.

**Scenario 13** (Insurance)**.** *The ScrupuleFree supermarket chain uses Bluetooth tracers to follow customers in its stores [11]. They link the Bluetooth identifier with real identified derived from the MyScrupuleFree app, or from bank cards used during checkout. While Mr. Smith is shopping, the company can simulate contact with his phone, so they will be notified if Mr. Smith is sick. This information will be sent to the insurance department.*

**By cyber criminals.** The proliferation of organised computer attacks over the past few years has been enough to convince us that organised cyber criminals could also try to retrieve this information.

**Scenario 14** (Malware)**.** *Mrs. Jones installed the CuteKittens app on her phone, without knowing that it is spyware (i.e. malware) that spies on her. After declaring in TraceVIRUS that she is sick, she receives a message to blackmail her, threatening to reveal her illness to her insurance company and her employer, who could terminate her employment during its probation period.*

Another lucrative organised-crime activity, very easy to implement in some of the tracking systems proposed, consists of triggering, for a fee, the compulsory quarantine fortnight of targeted people.

**Scenario 15** (Sale of positive alerts)**.** *Don Covideone sells an InfectYourNeighbour app on the Internet. After downloading the app, you just have to approach someone's phone for them to receive a notification that they are at risk. Attacks are now possible without technical skill. Thus, Mr. Bouque-Maeker intends to bet during the next Champion's League match. Luckily for him, he will attend the Gronaldo press conference. He then bets heavily on the opposing team, despite the 10-1 odds. He downloads the InfectYourNeighbour application and ensures his phone is near Gronaldo during the interview. Gronaldo receives an alert, he will not be able to play the game. His team loses and Mr. Bouque-Maeker wins!*

A malicious application of this type would work thanks to transmitters or receivers close to people who may be infected (near a medical laboratory for example). Then it just relays the messages between potentially-infected people and the person you wish to report as being at risk. This can be implemented in several of the proposed tracking systems (for example: very easily for DP3T, and with a little more technology for ROBERT).

## Conclusion

Tracing contacts poses many security issues and ones related to privacy, and the few scenarios that we have presented illustrate a small number of possible problems.

In this respect, cryptography can only deal with a limited number of these issues. A number of the situations that we have presented exploit the functionalities of this type of system, rather than their implementation. Therefore, judgements related to these risks cannot be resolved by technology, but necessitate making political choices that will balance foreseeable rights abuses and fundamental freedoms, and the potential benefits that can be expected in the fight against the epidemic. To our knowledge, the benefits conferred from digital tracing is still very uncertain today, while the scenarios that we have developed here are known and plausible. An essential principle in computer security is that the safety of a system should in no case rely on the assumed honesty of those involved in its creation, use, or management. This same principle appears in the evolution of our law in matters of protection of personal data. If, with the "Computing and freedoms" law of 1978, abuses were feared from the public authorities (particularly the State), followed by the private sector and then, subsequently through the GDPR, all members of society have been associated with these concerns. The attacks that a tracking system can make on the rights and freedoms of each and every one of us can come not only from the public authorities, which recommend its development and implementation, but also other people, collective or individual, who will learn how to take advantage of the many flawed properties of these systems. The first paragraph of section 1 of the 1978 Act has survived all of its revisions and developments. The urgency that we feel collectively in the face of our current situation should not make people forget: *Information technology must be at the service of every citizen. [. . . ] it should infringe neither on human identity, nor on human rights, nor on privacy, nor individual or public freedoms.*

## Références


[1] Ross Anderson. Contact tracing in the real world. https://www.lightbluetouchpaper.org/2020/04/12/contact-tracing-in-the-real-world/. (Published and consulted 12/04/20)

[2] Susan Landau. Looking beyond contact tracing to stop the spread. https://www.lawfareblog.com/lookingbeyond-contact-tracing-stop-spread. (Published 10/04/20, consulted 14/04/20)

[3] Bruce Schneier. Contact tracing COVID-19 infections via smartphone apps. https://www.schneier.com/blog/archives/2020/04/contact_tracing.html. (Published and consulted 13/04/20)

[4] Serge Vaudenay. Analysis of DP3T. Cryptology ePrint Archive, Report 2020/399, 2020. https://eprint.iacr.org/2020/399.

[5] Pascale Fombeur. Un decret d'application ne peut renvoyer a un arrete ulterieur la mise en œuvre des principes de la loi. AJDA, page 831, 2000.

[6] Alan Hunt. Explorations in Law and Society. Toward a Constitutive Theory of Law. New York, Routledge, 1993.

[7] La Quadrature du Net. Nos arguments pour rejeter StopCOVID. https://www.laquadrature.net/2020/04/14/nosarguments-pour-rejeter-stopcovid. (Published and consulted 14/04/20)

[8] Frederic Pierru. Les recompositions paradoxales de l'Etat sanitaire fran¸cais. Transnationalisation, etatisation et individualisation des politiques de sante. Education et Societes, 2012/2(30):107–129, 2012.

[9] John Hering, James Burgess, Kevin Mahaffey, Mike Outmesguine, and Martin Herfurt. Long Distance Snarf, August 2004. https://trifinite.org/trifinite_stuff_lds.html (18/04/20)

[10] Ben Seri and Gregory Vishnepolsky. The dangers of Bluetooth implementations: unveiling zero day vulnerabilities and security flaws in modern Bluetooth stacks.

[11] Michael Kwet. In stores, secret surveillance tracks your every move, June 2019. https://www.nytimes.com/interactive/2019/06/14/opinion/bluetoothwireless-tracking-privacy.html. (Consulted 18/04/20)

[12] Wikipedia. Scandale Facebook-Cambridge Analytica, 2020. http://fr.wikipedia.org/w/index.php?title=Scandale_Facebook-Cambridge_Analytica, (Consulted 18/04/20)