Perspective

Inherent privacy limitations of decentralized contact tracing apps

Yoshua Bengio,1,2 Daphne Ippolito,3 Richard Janda,4 Max Jarvie,5 Benjamin Prud’homme,2 Jean-François Rousseau,6 Abhinav Sharma,7 and Yun William Yu8

1Université de Montréal, Montreal, Quebec, Canada, 2Montreal Institute for Learning Algorithms, Montreal, Quebec, Canada 3Department of Computer and Information Science, University of Pennsylvania, Philadelphia, Pennsylvania, USA, 4Faculty of Law, McGill University, Montreal, Quebec, Canada, 5Borden Ladner Gervais LLP, Montreal, Quebec, Canada, 6Libero, Quebec City, Quebec, Canada, 7Centre for Outcome Research and Evaluation, McGill University Health Centre, Montreal, Quebec, Canada, and 8Computer and Mathematical Sciences, Instructional Centre 343, University of Toronto at Scarborough, Toronto, Ontario, Canada

Corresponding Author: Yun William Yu, PhD, Computer and Mathematical Sciences, Instructional Centre 343, University of Toronto at Scarborough, 1265 Military Trail, Toronto, ON M1C 1A4, Canada; ywyu@math.toronto.edu

Received 11 June 2020; Revised 17 June 2020; Editorial Decision 22 June 2020; Revised 17 June 2020; Accepted 23 June 2020

ABSTRACT

Recently, there have been many efforts to use mobile apps as an aid in contact tracing to control the spread of the SARS-CoV-2 (severe acute respiratory syndrome coronavirus 2) (COVID-19 [coronavirus disease 2019]) pandemic. However, although many apps aim to protect individual privacy, the very nature of contact tracing must reveal some otherwise protected personal information. Digital contact tracing has endemic privacy risks that cannot be removed by technological means, and which may require legal or economic solutions. In this brief communication, we discuss a few of these inherent privacy limitations of any decentralized automatic contact tracing system.

Key words: contact tracing, privacy, COVID-19, phone app

The advent of the coronavirus disease 2019 (COVID-19) pandemic has seen widespread interest in the potential utility of automatic tracing apps,1,2 as well as concern over their potential negative effects on individual privacy.3 By definition, contact tracing involves giving up some individual privacy, and it is important to carefully understand those privacy/utility trade-offs. In traditional manual contact tracing, a lot of personal information about both the diagnosed individual and exposed contacts is revealed to the central authority, including names, phone numbers, and locations of exposure. Decentralized automatic contact tracing apps do not require giving all of that information to a central authority but present other privacy challenges.

Individual privacy is broadly recognized as important for different reasons and by different constituencies. For some, it is an end goal in and of itself; others regard it as a fundamental desideratum for democratic institutions and for the proper functioning of civil society. It is also widely recognized, however, that many systems beneficial to individuals, democratic institutions, and civil society cannot function without some degree of access to personal information. To satisfy these competing objectives, legal frameworks have been deployed in many jurisdictions to set ground rules for how personal information is to be handled (eg, the General Data Protection Regulation in Europe; Health Insurance Portability and Accountability Act in the United States; Personal Information and Electronic Documents Act in Canada). One aim that is consistent across these various regimes is the emphasis on adequate security safeguards: when organizations and institutions collect, use, and disclose personal information, the systems put in place to facilitate these activities should minimize the potential for unauthorized access, thereby minimizing the possibility of unintended use.4
For automatic tracing apps that are focused on individual privacy, fulfilling these legal obligations is a basic first step. Enforceable privacy and data protection laws can provide some level of assurance to individual users that their personal information will not be unduly exposed. Yet compliance with such laws is still only a first step, for in the context of automatic tracing apps intended for general deployment across large populations of individuals, it is not clear that simple adherence will be sufficient. Automatic contact tracing apps generally depend on both sides of the contact (diagnosed and exposed persons) having the app installed, so user adoption is critical for the contact tracing to work. In countries where installation of such apps is voluntary, users may choose not to install an app if it leaks too much personal information. As such, many apps have gone beyond what is legally required and developed privacy protocols that aim to decentralize processing, storage and system control, and more generally decrease the amount of trust users need to invest in the app and the entities behind it.

Even with such controls, there remain residual privacy risks to all decentralized contact tracing systems. We believe that it is of paramount importance to acknowledge and analyze these inherent risks, allowing both end users and policymakers to make voluntary and informed decisions on the privacy trade-offs they are willing to tolerate for the purposes of fighting the COVID-19 pandemic. For end-users in particular, the legal basis for using personal information in contact tracing is founded on consent. It is therefore important that information about inherent risks is made generally available in order to support the meaningfulness of the consent obtained.

Let’s consider the most basic properties that any automatic decentralized contact tracing app must have: (1) when 2 phones are within a few meters of each other, a “contact” is recorded; and (2) when a user (Bob) has a change in COVID-19 status, all of his contacts (who we’ll refer to as Alice) over the past 14 days are notified of that exposure—note that Alice is simply informed of an exposure in the past 2 weeks, and may not be told the exact date. In practice, apps may use some combination of GPS, Bluetooth, or Ultrasound to achieve these aims, and the specific technologies used to determine the exposure may leak additional information, such as the date of exposure. However, the privacy leakages we describe here are agnostic to the technology used.

The inherent privacy leakages arise because, implicitly, Bob is sending information about his COVID-19 infection status to contacts based on colocation—while many apps do not directly use location information, contacts are still determined by Bob being in close proximity with another user, so the very existence of a contact event reveals some small amount of location information. An attacker who has sufficient information about or control over Bob’s location history can perform a linkage attack—that is, linking together external information with the messages Bob sends—to learn Bob’s infection status. Alternatively, sending notifications to Bob’s contacts may also reveal information about Bob’s location history if those notifications are too specific to him. An extreme case is if Bob is the only COVID-19 positive individual in a region, making a linkage attack trivial.

Businesses that have access to any part of Bob’s location history can gain access to his diagnosis status by placing a contact tracing device in his path. One concrete example of such a business is a hotel. In the simplest version of the attack, the hotel places a different phone running the contact tracing app in every hotel room every night. If Bob stays in Room 34 on June 1 and later sends his COVID-19 status, then the phone that was in Room 34 on June 1 will receive that message. Because the hotel knows the guest register, they are easily able to link that message to Bob, breaching his medical privacy.

This simple version of the attack can be thwarted by not allowing the hotel to run numerous instances of the app, perhaps by validating that every single copy of the app is associated with a real person or a real phone number. However, that does not block a more sophisticated binary-search version of this attack. Suppose that the hotel has 100 rooms and only 11 phones running the app—for example, they have 11 employees each with validated accounts. Then, at night when all the guests are in bed, each employee walks past half of their doors, only turning on their phone at specific doors for 15 minutes, creating an 11-bit code for each room/day pair. If employees 1, 3, and 5 walked past Room 34 on June 1, then the code would be 10101000000. Because an 11-bit code has $2^{11} = 2048$ possibilities, each of the 1400 room/day pairs can get a unique code. Later, if exactly employees 1, 3, and 5 receive messages, the hotel can conclude the message was from Bob. This may seem logistically challenging to coordinate, but it can be simulated synthetically with a hacked device in each room. These devices are no longer running the app as normal—so they might be considered illegal—but because they are simulating the behavior of a real person walking past rooms in a weird pattern, they cannot be technologically prevented. All a hotel needs is access to 11 accounts.

Although we have described this attack in the context of a hotel and a fixed location, this style of attack allows any malicious vigilante—let’s call her Mallory—to determine when and where she was exposed. There are 1344 fifteen-minute time intervals in a day; much like the hotel assigned an 11-bit label to each room, Mallory can assign an 11-bit label to each of those 15-minute periods to determine when she was exposed. If Mallory knows who she was in close proximity to during that 15-minute period, she may be able to reveal Bob’s COVID-19 status.

In practice, many proposed contact tracing protocols do not require using multiple identities because they do not require user validation when users are attempting to determine their own exposure status. For example, in several decentralized proposals being implemented, all of the contact matching happens locally on the phone. This is extremely powerful for protecting the user privacy of non-diagnosed users, as those users do not transmit any information off their phones, but it also means that there is no straightforward way to prevent an attacker from locally matching on multiple phones.

Suppose that Mallory wants to gain Bob’s location information, rather than his COVID-19 medical status. When Bob sends his COVID-19 status to contacts, Mallory receives a notification for every one of her encounters with Bob because there is no way for Bob to know that he met Mallory multiple times. If Mallory receives all her notifications from Bob around the same time, Mallory might be able to infer that all of her exposure notifications were likely for the same person, giving her a partial record of Bob’s movements because she knows who her path intersected with Bob’s. Of course, this can be made more difficult by not having Bob send all the notifications at once, but if exposure notifications are rare—for example, Bob is the only COVID-19-positive individual in a city—Mallory might still gain partial information.

The danger of the location history tracking is heightened if a large institution is the adversary, who we’ll call Grace. If Grace deploys phones around a city, she might be able to correlate together location histories of many diagnosed individuals. The reason Grace is able to do this despite receiving notifications from many individuals simultaneously is that she can sometimes acquire spatially and
temporally contiguous messages. If Bob was on Main and 1st, walking to Main and 2nd, and Grace has phones at both intersections receiving Bob’s notifications, she can infer that Bob sent both messages unless sufficient temporal noise is added in the moment of sending risk messages to past contacts. Of course, this information is comparable to that achievable through CCTV recording and face recognition without the use of any app, and furthermore, many smartphone users are already revealing detailed location histories to commercial services; thus, although strictly speaking contact tracing may leak location information, it is perhaps less worrying than medical information leaks.

In conclusion, automatic contact tracing holds the potential for greatly assisting in the fight against COVID-19. However, even with the best-designed systems, there are inherent limitations in how private a system can be technologically made, because identifying contacts’ COVID-19 status is the entire point of contact tracing. A privacy maximalist would rightly consider these attacks to be a reason to not use any decentralized automated contact tracing system. However, even privacy pragmatists may be concerned about the trade-off of revealing sensitive medical information like the COVID-19 status to businesses they frequent and strangers they encounter.

As technological solutions can only go so far, resolving the impact of many of these attacks is thus a matter of policy and law. To the extent that existing laws are not robust enough to address the automatic tracing app context, augmentations to existing legal frameworks may help to protect user privacy against legitimate central authorities, such as public health agencies, and deter private sector organizations, such as hotels, that might be tempted to leverage such attacks. Another potential mitigation is to change the economic incentive structure for legitimate actors. If a public health app deliberately provides partial hotspot information to a hotel, properly de-identified and spatially coarsened, that may be sufficiently useful to the hotel, depending on the economic motivations the hotel has for tracking individuals; coupled with legal restrictions, this could defend against businesses attempting to re-identify individuals.

Regardless, we believe that it is essential that designers and purveyors of contact tracing apps are transparent with the types of privacy guarantees they can offer. We authors have ourselves proposed a decentralized automated contact tracing app design, and this brief communication is helpful in clarifying the baseline privacy trade-offs that all decentralized automatic contact tracing systems are asking users to make. It is only with informed consent and transparency that automatic contact tracing efforts will be successful in helping fight the COVID-19 pandemic.

AUTHOR CONTRIBUTIONS

The content of this manuscript arose from discussions among the listed authors during the design and development of the COVI contact tracing app. RJ, YB, DI, and YWY realized the need for transparency in privacy trade-offs. JFPR conceived the hotel attack scenario. YWY analyzed the binary search and location tracking approaches. MJ, BP, and AS provided respectively the legal, societal, and medical contexts for the manuscript. All authors were involved in the drafting of the manuscript.

CONFLICT OF INTEREST STATEMENT

YWY reports funding from the Toronto COVID-19 Action Initiative for this work. AS reports grants from Fonds de la Recherche en Sante du Quebec—Junior 1 clinician scientist programme and Bristol-Myers Squibb-Pfizer; personal fees from Novartis and AstraZeneca; and grants and personal fees from Roche Diagnostics and Boehringer-Ingelheim, outside the submitted work. The authors are part of a team developing the “COVI” COVID-19 risk awareness application.

REFERENCES