The Social, Legal And Ethical Implications Of Cryptography In Covid-19 Contact Tracing

Jounaid Ruhomaun, December 2020

Abstract

This report documents an analysis of the ideas presented around the topic of COVID-19 contact tracing applications within the following media article (published in May 2020): *'Coronavirus contact-tracing apps: can they slow the spread of COVID-19?' (Zastrow, 2020),* with additional reference and analysis of more recent publications. Discussion within this report is in regards to the social, legal and ethical implications of cryptography use within such applications.

Introduction

Given that traditional contact tracing is considered a very labours and slow human process, it can potentially be seen as somewhat ineffective at controlling a pandemic at the national level, due to the fast and unpredictable developments in local outbreaks. Therefore automated contact tracing systems can be highly beneficial in terms of efficiency as these systems would reduce the human factors such as in-person interviews and detective work *(Zastrow, 2020)*. Due to the fact that in the modern day smartphones are widely distributed throughout most first world societies, they are considered an essential tools in the development of automated contact tracing networks. Therefore most, if not all of the automated contact tracing systems involve some form of mobile application that collects and shares data on its userbase with regards to potential exposure of the virus.

Bluetooth Contact Tracing

The two generally accepted designs for an automated contact tracing network are the centralised system, and decentralised system models. The first stage in both models is the transfer of a key between users of the application when they come in close proximity of one another *(Zastrow, 2020)*. This is generally done by broadcasting a Bluetooth signal between users devices, with its signal strength determining whether said users were in close enough proximity (for a defined amount of time) in which the virus could potentially have been contracted *(Greenberg, 2020)*. This is referred to as a 'contact event'.

There are obvious data protection concerns around the potential for malicious entities to trace certain users, therefore a cryptographic system was developed by Google and Apple to ensure the privacy of users *("Contact Tracing Cryptography Specification", 2020)*. The basic principle is to use three keys (each generated from the previous), one tracing key that is stored privately for each user, one daily key that is generated every 24 hours and is shared with trusted authorities upon a positive COVID-19 result, and a rolling identifier key that is exchanged between users (that changes every 10 minutes). This results in a user's identification to be traceable by others for only 10 minutes, heavily increasing user privacy. Since this protocol is directly embedded into the Android and IOS operating systems, it can be considered safe from any (potentially malicious) third party applications on the device *(Buchanan, 2020)*. Some however might still have concerns with this system simply due to the fact it was developed by private companies rather than their own governments.

Centralised vs Decentralized Systems

The decentralised model takes the approach of only uploading the list of contact event pseudonyms from a user given a positive COVID-19 test result, to a central database. Other user's applications will frequently download a copy of said list, and cross reference against its own recorded contact event data, and alert the user upon receiving a match *(Zastrow, 2020)*. In this approach there is no specific location or proximity data shared, and all the processing is done on each device individually, so even if the central database were to be compromised malicious entities would not have access to any personally identifiable/traceable information (given the three key approach: *Buchanan, 2020*). Therefore, the privacy of all users is ensured, as Stanford computer scientist Cristina White suggests, "The best way to protect geolocation data from abuse, is not to collect it in the first place" *(Greenberg, 2020)*. However, since every single contact event would result in notification, critics of this model argue about its efficacy in nations without widespread testing capability *("Covid Contact tracing apps are a complicated mess: what you need to know", 2020)*.

In the centralised model, given a positive test result the user's contact event data, as well as possible location and other proximity/interaction data, are uploaded to a central authorities server, where an algorithm determines which users to notify based on said data *(Zastrow, 2020)*. Proponents of such a model suggest that since testing at the beginning of the pandemic wasn't done with ease, the centralised approach would be more effective (in comparison to the decentralised model) as only those deemed necessary would be contacted by the system to get tested, whilst also having sufficient data to provide additional epidemiological insights such as revealing clusters and super-spreaders *("Covid Contact tracing apps are a complicated mess: what you need to know", 2020).*

Issues Presented by the Centralised Model

There are obvious security concerns with the centralised approach, as even if all personally identifiable location and time data were to be stored cryptographically, if the system were to become compromised this data would be easily decipherable through 'hash cracking' (as is commonly practiced with password cracking: *Porup, 2020*). The 'Private Kits: Safe Paths' project developed by MIT presented a solution to this by redacting identifiable locations and replacing them with 'tiles' (of a few square miles) which are hashed along with time information, making the information no longer personally identifiable, whilst also still being able to track the pandemics developments at local levels *(Greenberg, 2020)*. This approach provides an ethical compromise between privacy and useful data to help control the pandemic.

However, despite these cutting edge cryptographical innovations that were developed around the beginning of the pandemic, later analysis of the applications that were eventually implemented suggests the majority were developed with a disregard for cryptographical security *(Zorz, 2020)*. This was observed in the original application that was being developed by NHSX in the UK, where it was decided to not to use the previously described 'three key' system embedded within IOS and Android operating systems, and only using a daily generated random ID, which would have increased the chance of user traceability. The application design was also criticized for storing unencrypted data that could potentially be used to determine when certain users met with one another *("Coronavirus: Security flaws found in NHS contact-tracing app", 2020)*. NHSX later decided to backtrack and adopt a decentralised model based on Google/Apple's API due to these issues *(Downey, 2020)*.

Another concern is the potential for functionality creep, and for more authoritarian governments and institutions to use such technology to increase civilian surveillance *(Zastrow, 2020)*. Such authorities could increase the breadth of data collected by these contact tracing systems, and continue implementation well after the pandemic has concluded as a way of exerting extra control over its populace. Such unlawful practice was observed by the government of Israel, that seized telco data containing information about all its citizens interactions and movements (including those without COVID-19 contraction, or even symptoms), and handed said data to its intelligence agency to process. Israel's supreme court responded by stating it was absolutely clear those actions were unconstitutional and an intentional power grab, for which they introduced new regulation to prevent further unlawful developments *("Coronavirus: Israeli court bans lawless contact tracing", 2020)*.

The Ethical Dilemma of Preserving Both Privacy and Lives

Privacy and data protection is always a highly debated topic around the development of new technologies, however, in this specific situation such debate could potentially cost lives *(Zarei, 2020)*. Due to the nature of viruses, it was imperative that national health authorities gained a verbose model detailing the spread of COVID-19 quickly and as early on in the pandemic as possible, in order to carry out sufficient action that would save lives. If automated contact tracing technologies were developed with no concern for privacy and data protection, they potentially could have been implemented much faster, providing necessary epidemiological data earlier on in the pandemic. This presents the following question in hindsight: was it really ethical to spend time debating and developing contact tracing applications around privacy concerns as people were actively dying due to a lack of epidemiological information?

One country that took somewhat authoritarian contact tracing measures early on was South Korea. Having had experienced a national outbreak of MERS in 2015, they were more prepared in regards to how COVID-19 would spread. The countries national assembly allowed for the government to collect information such as mobile phone location data from infected citizens. This data was reconstructed into detailed models of the infected persons movements, which was subsequently released to the public *(Zastrow, 2020)*. Despite initially being one of the worse affected countries in terms of COVID-19 cases back in February/March 2020, their measures lead to them only having 564 confirmed deaths as of December 1st 2020, compared to the UK with a similar population, currently (as of December 1st 2020) at 59,051 confirmed deaths *("CSSEGISandData/COVID-19", 2020)*.

Efficacy Requires Social Trust and Acceptance

Unlike in nations such as China and Hong Kong where citizen participation in their contact tracing system is mandatory *(Gamvros, Evans, Cwalina & Flockhart, 2020)*, western nations that highly value personal freedoms (such as the United States and United Kingdom) must persuade the majority of its populace to partake In such systems. Research carried out at the University of Oxford suggests that at least 60% of a populace needs to partake in contact tracing in order to control an outbreak *(Zastrow, 2020)*. Such western societies generally view privacy (especially from the government) with high importance, therefore its essential for such authorities to be transparent about what data is collected, and what cryptographical measures are in place in their contact tracing systems (despite the possible ethical implications discussed previously).

An example of where poor government decisions lead to potential social mistrust was when it was revealed that the original contact tracing application being developed for the UK by NHSX wouldn't be implementing Google/Apple's 'three key' cryptographic system (for which the decision was later changed: *Andrea, 2020*), despite it being highly praised *(Zastrow, 2020)*. This could have potentially lead to less of the UK's populace trusting any future application developed by NHSX, which would result in the systems efficacy being greatly diminished.

The Potential for Certain Societal Groups to be Unincluded

Another social factor that would reduce the efficacy of application based contact tracing systems is the simple fact that not every citizen in a populace has access to a smartphone *(Zastrow, 2020)*. A study carried out by Ipsos MORI around the final released iteration of the NHSX application suggested that those who were most vulnerable to COVID-19 were less likely to download and use the app, and that certain societal groups weren't even aware of the application *(Loughran, 2020)*. This suggests a fully automated contact tracing system could be deemed as being unethical and discriminatory, despite the benefits it would provide.

An example that highlights the potential for inequality in these systems was when the Indian government decided to make their application based contact tracing mandatory for its entire populace *("Covid Contact tracing apps are a complicated mess: what you need to know", 2020)*. India is a nation with immense inequality and a large wealth divide, where a many of its citizens don't even own a mobile device let alone a smartphone. Therefore this decision perplexed the international community, and given India's history with police brutality, there was the potential for possible human rights violations.

Contact Tracing and Western Law

Regardless of the approach taken to automated contact tracing, western authorities generally have laws in place which inevitably affect the way in which these systems can be implemented. An analysis of Google/Apple's Bluetooth contact tracing protocols against certain western data protection laws suggest these regulations can either be a hinderance, or an advantage in regards to the development of such systems *(Bradford, Aboy & Liddell, 2020)*. The article suggests that narrow, sector specific regulation such as that of the United States HIPAA act of 1996 *(Ladenheim, 1997)* and the CCPA act of 2018 *(Goldman, 2018)*, are insufficient in providing useful guidelines for the development of such systems, whereas more broad regulation with expansive scope such as the EU GDPR law *(Nahai, 2018)* provide a functional blueprint for the development of contact tracing systems, that is compatible with fundamental rights. Despite this, the UK government managed to break GDPR law whilst implementing their contact tracing application, as unredacted personally identifiable information was shared in training material *(Marsh & Hern, 2020)*. This suggests that even verbose and well regarded law that is meant to ensure the protection of citizens privacy can easily be disregarded, even by government agencies.

Conclusion

To conclude, it is apparent that there are numerous social, legal and ethical implications around the recent development of automated contact tracing systems. Privacy and data protection should be taken into account to promote social trust in the system, as its efficacy relies heavily on user participation. This can be done through the use of secure and transparent cryptographic techniques, as with Google/Apples 'three key' system. However, more authoritarian governments could use these technologies as an excuse to increase control and surveillance over its citizens, even after the pandemic has concluded, which could result in long term effects. Overall, since COVID-19 is the first pandemic to play out in this digital era, it is important that modern technologies are utilised to their fullest in order to help control the spread of the virus, as human lives are at stake.

Bibliography

Zastrow, M. (May, 2020). Coronavirus contact-tracing apps: can they slow the spread of COVID-19?. Retrieved 2 December 2020, from https://www.nature.com/articles/d41586-020-01514-2

Greenberg, A. (August, 2020). Clever Crypto Could Protect Privacy in Covid-19 Contact-Tracing Apps. Retrieved 2 December 2020, from https://www.wired.com/story/covid-19-contact-tracing-apps-cryptography/

Contact Tracing Cryptography Specification. (April, 2020). Retrieved 2 December 2020, from https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ContactTracing-CryptographySpecification.pdf

Buchanan, B. (April, 2020). Contact Tracing: The Most Amazing And Scariest Technology of The 21st Century. Retrieved 3 December 2020, from https://medium.com/asecuritysite-when-bob-met-alice/contact-tracing-the-most-amazing-and-scariest-technology-of-the-21st-century-9fb86d7869e5

The security behind the NHS contact tracing app. (May, 2020). Retrieved 4 December 2020, from https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app

Covid Contact tracing apps are a complicated mess: what you need to know. (May, 2020). Retrieved 4 December 2020, from https://privacyinternational.org/long-read/3792/covid-contact-tracing-apps-are-complicated-mess-what-you-need-know

Porup, J. (May, 2020). Hashcat explained: How this password cracker works. Retrieved 4 December 2020, from https://www.csoonline.com/article/3542630/hashcat-explained-why-you-might-need-this-password-cracker.html

Coronavirus: Israeli court bans lawless contact tracing. (2020). Retrieved 4 December 2020, from https://www.bbc.co.uk/news/technology-52439145

Zorz, Z. (June, 2020). Most COVID-19 contact-tracing apps are not adequately secured - Help Net Security. Retrieved 4 December 2020, from https://www.helpnetsecurity.com/2020/06/18/contact-tracing-apps-security/

Coronavirus: Security flaws found in NHS contact-tracing app. (2020). Retrieved 4 December 2020, from https://www.bbc.co.uk/news/technology-52725810

Zarei, K. (July, 2020). Digital Contact Tracing Efforts Hampered by Privacy Concerns. Retrieved 4 December 2020, from https://www.govtech.com/health/Digital-Contact-Tracing-Efforts-Hampered-by-Privacy-Concerns.html

CSSEGISandData/COVID-19. (2020). Retrieved 4 December 2020, from https://github.com/CSSEGISandData/COVID-19

Gamvros, A., Evans, M., Cwalina, C., & Flockhart, F. (May, 2020). Contact tracing apps in China, A new world for data privacy. Retrieved 4 December 2020, from https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/china-contact-tracing.pdf?revision=249d55f4-eb9a-49dd-8491-b8c9c7626691&la=en-cn

Downey, A. (September, 2020). NHS Covid-19 contact-tracing app launched in England and Wales. Retrieved 4 December 2020, from https://www.digitalhealth.net/2020/09/nhs-covid-19-contact-tracing-app-launched-england-wales/

Loughran, J. (September, 2020). Covid-19 contact tracing app effectiveness questioned one day before launch. Retrieved 4 December 2020, from https://eandt.theiet.org/content/articles/2020/09/covid-19-contact-tracing-app-effectiveness-questioned-one-day-before-launch/

Bradford, L., Aboy, M., & Liddell, K. (May, 2020). COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes. *Journal Of Law And The Biosciences*, *7*(1). doi: 10.1093/jlb/lsaa034

Ladenheim, K. (1997). Health Insurance in Transition: The Health Insurance Portability and Accountability Act of 1996. *Crossref Listing Of Deleted Dois*, *27*(2), 33. doi: 10.2307/3330636

Goldman, E. (2018). An Introduction to the California Consumer Privacy Act (CCPA). *SSRN Electronic Journal*. doi: 10.2139/ssrn.3211013

Nahai, F. (2018). General Data Protection Regulation (GDPR) and Data Breaches: What You Should Know. *Aesthetic Surgery Journal*, *39*(2), 238-240. doi: 10.1093/asj/sjy296

Marsh, S., & Hern, A. (July, 2020). Government admits breaking privacy law with NHS test and trace. Retrieved 4 December 2020, from https://www.theguardian.com/technology/2020/jul/20/uk-government-admits-breaking-privacy-law-with-test-and-trace-contact-tracing-data-breaches-coronavirus