Covid-19 Crisis: Is our personal data likely to be breached?

Vinden Wylde, Edmond Prakash, Chaminda Hewage and Jon Platts
Cardiff School of Technologies
Cardiff Metropolitan University, Cardiff, Wales, UK
{vwylde | eprakash | chewage | jplatts} @cardiffmet.ac.uk

1 Introduction

Since the Coronavirus (SARS-Cov-2: Covid-19) outbreak, the pandemic of 2020, mobile Applications (apps) via the Internet of Things (IoT: smart-phones, sensors and devices) and Internet of Everything (IoE: Cloud and Phone networks) continue to play a key role in tracking and tracing programs. Many countries seek different approaches to minimise person-person transmission [1, 2]. However, perspectives of the privacy paradigm shift with recent privacy implications arising from the urgency in deploying digital solutions, demonstrate in pandemic times how people's data privacy is at higher-risk of breach, and that data acquisition and it's handling [of an individuals personal data] has become a more vibrant research area as a consequence [3]. However, it is not simply a matter of utilising technology to mitigate risk, but a partnership between technology, policy and a given population that will enable consistency, proportionality and transparency in service delivery, thus help to build trust and enable scalability via the internet.

2 Test-trace-track Programs and Trust

2.1 Test-trace-track Apps

For example, in a survey conducted in the Republic of Ireland, over 8,000 participants generally accepted a contact tracing app (54% positive rate) , and from a similar survey of 2,000 respondents from the United Kingdom (UK), showed that government-controlled application acceptance/uptake was at 55%, with higher acceptance rates from the NHS controlled app [1]. This small piece of research demonstrates a lack of app uptake in the remaining 45% of the population which hinders a government's ability in effective collection, handling and processing of medical data.

However, in other countries, citizen consent is inferred if data collection is utilised for the public good [need no individual consent] where private parties' access to data is accepted by government. Amnesty International (2020) raised similar concerns regarding data privacy stating that contact tracing apps deployed in similar instances throughout numerous countries [1].

This further highlights the true scale of the problem and how data protection is perceived across the globe and in poorer countries, thus justifying the need for more collaborative research on data privacy. By the analysis of such varied legal frameworks, technical solutions and practices in mitigating data privacy risk in such a critical situation as a global pandemic, we can learn how best to apply swift, effective, scalable and powerful solutions. Moreover, it's clear that transparent systematic and robust data on the distribution of the Covid-19 vaccine for each nation is urgently needed [4].

2.2 Data Privacy Frameworks [UK]

A current example in the UK is the Data Protection Act 2018 (DPA) and General Data Protection Regulations 2016 (GDPR), which together regulate how personal data is utilised by businesses, organisations and governments and lays out 8 key objectives. Anyone responsible for handling of processing personal data must adhere to these strict principles which include that: data has to be lawful [acquisition], fair, accurate and up-to-date, not kept longer than needed, kept safe and secure, and not to be transferred outside the European Economic Area (EEA). The European GDPR was designed in alignment with human rights law which also lays out core principles for the processing of any collected data, its data-types, its intended purpose and the duration needed in its processing [5].

For example, in GDPR Recital 4 and in the proceeding Directive 1995/46/EC Recital 2, sum-up a main objective in that *"the processing of personal data should be designed to serve mankind"*. The core principles utilised by the Data Controller in ensuring compliance, the legal grounds and justification of data processing are, Necessity (not only processing convenience) and Proportionality. In processing high-risk health data for example, a mandatory Data Protection Impact Assessment (DPIA) is undertaken to establish and mitigate risk, and if the risk is not brought to an acceptable level, assess if the data should be processed at all [6].

This demonstrates a good example from how the UK and EU frameworks cooperate in alignment regarding data protection law, and shows inclusively with a robust, ethical and transparent method to control and mitigate risk in the context of data privacy. However, this also highlights the diverse movement of people [and legal frameworks] across the globe which should alarm governments, organisations and businesses in regard to data protection planning and strategy.

3 Perceived Challenges and Solutions on the road to Good Practice

3.1 NHS Test-Trace app: Transparency

As for the UK Government and NHS X (Digital NHS branch) in fighting the Covid-19 Pandemic aided by the private sector, digital contact tracing apps continue to generate controversy around its utility and compliance with GDPR. Companies that work on behalf of NHS X for example, can be considered as processors of data and therefore NHS X should obligate such companies in the provision of data protection. The NHS X app code and DPIA was voluntarily submitted to the Information Commissioners Office (ICO) without the data store, which in turn could bring into question the UK Governments overall comliance and surveillance capabilities. The Joint Committee on Human Rights (JCHR) for example, showed a cause for concern at the rapid deployment of contact tracing apps, more specifically their data protection regimen prior to its roll out in March 2020 [6].

3.2 Blockchain and Smart Contracts: Accountability and Traceability

Part of a solution here [government transparency] includes ongoing development of data privacy and accountability methods. In Antal (2021), the authors discuss how Blockchain (BC) technology can be utilised for tracing, transparency and assurance of Covid-19 vaccine registration, storage and delivery to include self-reporting (i.e. side effects). With this in mind, a BC implementation strategy is proposed in assuring data immutability and integrity with the provision of 'in case of beneficiary registration for vaccination' eliminating impersonations and identify theft [7].

In Honduras for example, a Toronto-based technology launched Civitas, an app which links a users' unique government-issued ID on a blockchain-based network. The BC stores data necessary for determining an individuals best time to go shopping for food or medicine, and enables government agencies in resource deployment strategies [8]. However, a weakness with regard to GDPR includes the right to be forgotten and processing speed. BC by design would be more suited in the governance and management of Big Data

repositories and warehouses, a relatively new and progressing data storage and management technology, which aided by a digital Smart Contract (SC) can enhance consistency with accountability in a transparent forum.

3.3 COVID-19: Vaccine Hesitancy in UK households

As a consequence to the Covid-19 pandemic, the UK started vaccinating it's population, whilst mass vaccination programs were also taking place globally, however vaccine hesitancy from historic mistrust in government and public health bodies, particularly in ethnic minorities, highlight disparities which show a lack of public engagement, understanding and trust in technology [9, 4]. Another more common reason for such hesitancy includes health effects (long-term) and trust in the vaccine itself. In a UK survey undertaken in December 2020, black, Bangladeshi and Pakistani populations showed the highest vaccine hesitancy rates when compared with the white ethnic populations [9]. Robertson 2021 states that *"Herd immunity may be achievable through vaccination in the UK but a focus on specific ethnic minority and socioeconomic groups is needed to ensure an equitable vaccination program."* [10]. This would include a more targeted approach to those with mental illness and with learning disabilities [11].

3.4 Data Storage and Identification

Another part of a solution involves clear definitions for data storage methods. At present, is extremely difficult to obtain a comprehensive and integrated view of (i) what personal data is using for storage from within an organisation, (ii) making sure that an organisation fully comprehend the regulation content and (iii) the production of the necessary records from data processing activities [5]. While GDPR compliance has enhanced the protection of personal data (i.e. Personal Identifiable Information (PII), sharing PII with add and marketing, collecting and sharing location, sharing PII of children, sharing with law enforcement, and data aggregation), it remains a challenge as more work is necessary, particularly in the areas of granting a users the right to edit, update, and delete their data to entirely fulfil the GDPR promise[12].

4 Conclusion

So. Is our personal data likely to be breached?

Given all the above-mentioned, how can the information provided [sometimes without consent] and collected from you and I in a global context be ethical, accurate and legible for an effective data collection, vaccine or delivery strategy? Clearly, only a small part of the puzzle is apparent in ultimately gaining the population's support in digital app uptake and in any future globally scalable test-trace/tracked vaccination deployment program. Therefore frameworks and outcomes need to be continually assessed, with organisations, governments and businesses planning for the long-term with strategies world-wide in scope, thus ensuring individual and group data privacy integrity in the cloud.

Although collecting, processing and deleting data are necessary components controlled by GDPR, educating and engaging with minorities and mental illness groups may encourage trust and provide future group reassurances. As demonstrated in different countries, some groups may be understandably unfamiliar with data protection concepts, which in itself provides an avenue for engagement in restoring national and international trust in overall future data protection efforts in a disaster or global emergency scenario. Additionally, the answer is not just robust technical solutions, but also the resources, operation, design and management of policy and practice, thus symbiotically enhancing data protection objectives, population trust/uptake and remedial actions globally.

Bibliography

[1] R. Raman, K. Achuthan, R. Vinuesa, and P. Nedungadi. COVIDTAS COVID-19 Tracing App Scale—An Evaluation Framework. *Sustainability*, 13(5):2912, 2021.

[2] J.S. Juneidi. Covid-19 Tracing Contacts Apps: Technical and Privacy Issues. *Int. J. Advance Soft Compu. Appl*, 12(3), 2020.

[3] A. Majeed. Towards Privacy Paradigm Shift Due to the Pandemic: A Brief Perspective. *Inventions*, 6(2):24, 2021.

[4] M. Black, A. Lee, and J. Ford. Vaccination against COVID-19 and inequalities–avoiding making a bad situation worse. *Public Health in Practice, Elsevier (Oxford, England)*, 2021.

[5] J. Tran and C. Ngoc. GDPR handbook for Record of Processing Activities. Case: The Color Club A/S, 2020.

[6] A. Guinchard. Our Digital Footprint under Covid-19: Should We Fear the UK Digital Contact Tracing App? *International Review of Law, Computers & Technology*, 35(1):84–97, 2021.

[7] C.D. Antal, T. Cioara, M. Antal, and I. Anghel. Blockchain platform for COVID-19 vaccine supply management. *arXiv preprint arXiv:2101.00983*, 2021.

[8] How Blockchain is helping in the fight against Covid-19. `https://www.lexology.com/library/detail.aspx?g=8b5ef0f0-05b3-4909-b5d5-da7bd57f0381`. Accessed: 24-04-2021.

[9] M. S. Razai, T. Osama, D McKechnie, and A. Majeed. Covid-19 vaccine hesitancy among ethnic minority groups, 2021.

[10] E Robertson, K.S. Reeve, C. L. Niedzwiedz, J. Moore, M. Blake, M. Green, S.V. Katikireddi, and M.J. Benzeval. Predictors of COVID-19 vaccine hesitancy in the UK Household Longitudinal Study. *Brain, behavior, and immunity*, 2021.

[11] B. MacKenna, H.J. Curtis, C.E. Morton, P. Inglesby, A.J. Walker, J. Morley, A. Mehrkar, S. Bacon, G. Hickman, C. Bates, et al. Trends, regional variation, and clinical characteristics of COVID-19 vaccine recipients: a retrospective cohort study in 23.4 million patients using OpenSAFELY. *medRxiv*, 2021.

[12] R.N. Zaeem and S.K. Barber. The effect of the GDPR on privacy policies: Recent progress and future promise. *ACM Transactions on Management Information Systems (TMIS)*, 12(1):1–20, 2020.