DOI: 10.1111/iwj.13807

EDITORIAL

IWJ WILEY

Data privacy and management - A COVID legacy or curse?

Following our last editorial[1] regarding the importance of data in the evolution and the potential impact of the coronavirus disease 2019 (COVID-19) intrusion, here we would like to expand on the impact that COVID-19, moving forward, is likely to have on the privacy aspects of data.

The COVID-19 pandemic led governments, globally, to use tracking technologies and other data driven tools to monitor and curb the spread of COVID-19.[2] Such large-scale intrusions into privacy and data protection are unthinkable during normal times. However, in times of a pandemic, the use of location data provided directly to government by technology companies becomes an accepted option.[3] For the most part governments, and the general population alike, accept such practices if in the name of public health.[4]

Established privacy rules and regulations are typically focused on individual consent.[2] We have recently witnessed how these can be overridden during states of emergency for the greater good of the population and humankind. Emergency use, often implemented in a short timeline with little testing, leaves poor with safeguards and guarantees of individual and collective privacy.[5] The challenge of responsible data use during a crisis is not novel, since this is not the first humanitarian crisis the world has faced, albeit is one of the most challenging. Governments and other research organisations have tried to use data responsibly under these extreme circumstances. But what will history show regarding this practice? What will come back to bite us in the proverbial behind?

The use of location data, to monitor and control the coronavirus pandemic, can be useful, improving the ability of governments and researchers to combat the threat more quickly. Can we and should we go beyond this in the name of public health? For example, genetic data can be relevant for vaccines and monitoring online communication might be helpful to keep an eye on peace and security, but where would it stop? However, the use of such large amounts of data comes at a price for individual freedom and collective autonomy.[5] The risks of the use of such data should ideally be mitigated through similar legal frameworks developed to control private data. This should include the purpose and objectives of data use, its collection, analysis, storage, and sharing, as well as its destruction once it is no longer required. However, during a crisis, do we have the time or will to ensure such parameters are met or followed?

Some of the key early findings of such practices during COVID-19[2]:

- *data sensitivity is highly contextual*; one and the same data can be sensitive in different contexts.
- *privacy and data protection are important values*; they do not disappear during a crisis. Nevertheless, they must be weighed against respective benefits and risks.
- *data-breaches are inevitable*; with such expediency of design and use, the chance of any system being hacked approaches 100%. Hence, it is not a question of whether, but when. Therefore, governments must prepare sound data retention and deletion policies.
- *data ethics is an obligation to provide high quality analysis*; that is to maximise the use of this data to provide the highest quality of analysis possible.

Data-driven practices must be used in a responsible manner, even during a pandemic.[6] So, we must learn the lessons of this crisis to evaluate our ongoing privacy policies and practices for the good of humankind. Sharing is caring. Furthermore, it will be important to observe whether data and surveillance practices introduced during the pandemic will be rolled back to status quo pre-COVID. Or will this experience herald a new privacy norm moving forward?

COVID CONDITIONING

Most if not all users of smart devices, which encompasses a huge percentage of the global population, are being constantly followed and tracked by large conglomerates.[7] We accept this as a way of life, or the cost of having the

device. But when government wants to do it for the benefit of mankind, it becomes an issue for debate and worry.

The acceptance of the conglomerate tracking is enhanced utility, connectivity, and societal interaction.[8] Isn't that the same for the COVID tracking apps? Why rely on your memory when it comes to your health and catching a potentially deadly virus? Let us face it our memories have become somewhat weakened by years of smart utility. How many of us can recite a family member's or a friend's phone number these days?

One specific example is, we will track our phone which for the most part is almost 100% of our movement as it is always with us. Our primary belief is the hope of locating it should we misplace it. It's kind of ironic that we will accept an "invasion of privacy" to find a lost phone but not to protect our health.

For those individuals choosing to have a smart device, there is little if any choice regarding acceptance of tracking behaviour.[9] Recent practice has been more choice in which apps track you and you can opt out, but the main tracking and geolocation remains and is a non-negotiable aspect of the device utility. Yet when government makes the use of contact tracing apps,[3] more necessary through coercive incentives for those who use it, we raise our hands in alarm.

The most important legacy of the pandemic will be a clearer understanding of not only data privacy but also everything that goes with it. Tied to this is perhaps a clearer understanding of humanity and its feelings towards data privacy. This is especially true in the healthcare arena where perhaps the new "technology-phillic" patients are more willing for data sharing if it benefits their health or the care provided by the healthcare system (eg, virtual health)?

Douglas Queen
Editor, International Wound Journal

REFERENCES

1. Queen D, Harding K. Data capture, analysis, utility and privacy and a COVID legacy. *Int Wound J*. 2022;19(3):465-466.
2. Zwitter A, Gstrein OJ. Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. *Int J Humanit Action*. 2020;5:4.
3. Gupta S, Nguyen T, Raman S, et al. Tracking public and private responses to the COVID-19 epidemic: evidence from state and local government actions. *Am J Health Econ*. 2021;7(4):361-404.
4. Frieden TR. A framework for public health action: the health impact pyramid. *Am J Public Health*. 2010;100(4):590-595.
5. Mantelero A. From group privacy to collective privacy: towards a new dimension of privacy and data protection in the big data era. In: Taylor L, Floridi L, van der Sloot B, eds. *Group Privacy. Philosophical Studies Series*. Vol 126. Cham: Springer; 2017.
6. Ienca M, Vayena E. On the responsible use of digital data to tackle the COVID-19 pandemic. *Nat Med*. 2020;26:463-464.
7. Allmendinger RW, Siron CR, Scott CP. Structural data collection with mobile devices: accuracy, redundancy, and best practices. *J Struct Geol*. 2017;102:98-112.
8. Bayoumy K, Gaber M, Elshafeey A, et al. Smart wearable devices in cardiovascular care: where we are and how to move forward. *Nat Rev Cardiol*. 2021;18:581-599.
9. Balebako R, Jung J, Lu W, Cranor LF, Nguyen C. (2013). "Little brothers watching you": raising awareness of data leaks on smartphones. Paper presented at: Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS'13). Association for Computing Machinery, New York, NY, USA, 12, 1–11.