Short Report

Asia Pacific Journal of Public Health
1–3
© 2020 APJPH
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1010539520984360
journals.sagepub.com/home/aph
SAGE

Using Big Data Tools to Analyze Digital Footprint in the COVID-19 Pandemic: Some Public Health Ethics Considerations

Olivia M. Y. Ngan, PhD[1] and Adam M. Kelmenson, MS[1]

Abstract

While many freedoms became halted by city lockdowns and restrictive travel bans amid coronavirus crisis, some countries and regions reopened with public health monitoring and surveillance measures in place. Technology applications such as real-time location data, geofencing technology, video camera footage, and credit card history are now used in novel and poorly understood ways to track movement patterns to stem viral spread. The use of big data analytics, which sometimes involve involuntary and unconsented data access and disclosure, raise public unease about data protection. The result is a balance between public health safety and ethical use of personal data that pushes the limits of privacy rights. Is it ethically permissible to use big data analytics instantiating the goal of public health by infringing on personal privacy in exchange for maximizing public security? Demonstrating the effectiveness of public health measures is difficult as scientific uncertainties and social complexities are presented. This article provides some public health ethics considerations in balancing benefits of public security and personal privacy infringement, supported with examples drawn from Asian countries and regions.

Keywords

big data, digital technology, public health surveillance, public health ethics, ethics

What We Already Known

- Digital contact tracing and surveillance were adopted in the COVID-19 pandemic, underscoring the importance of data protection and privacy.
- Weighing individual privacy against public health resulted in a heated debated in the context of big data and pandemic.

What This Article Adds

- This article provides some public health ethics considerations in balancing benefits of public security and personal privacy infringement
- Big data tools become more resilient in a long-run and what purposes could be served in the post-COVID-19 era should be discussed in an open and transparent manner.

Commentary

In China, the government utilized a national e-wallet application as surveillance tools to link digital footprints, such as transports and purchase records to indicate who showed potential interactions with an infected person. In Singapore, a smartphone application monitored the transmission by contact tracing and location check-in/check-out systems.[1] When data show that an individual was close to someone who has tested positive for the virus, or in a location with confirmed cases, the users can send logs to the government and receive serological tests. In Taiwan, the health database is connected with the customs database to generate real-time alerts based on travel history and symptoms to aid case identification.[2] Increasing numbers of countries adopted similar measures,[1,3,4] reflecting a consensus that big data analytics are pivotal in supporting outbreak management. However, the adoption of such measures by the general public, either by choice or by mandate, vary by regions.

The following analyzes the ethics of data usage in the pandemic grounded on the principle of double-effect using constellation public health values. The principle of double-effect

[1]CUHK Centre for Bioethics, The Chinese University of Hong Kong Faculty of Medicine, Hong Kong

Corresponding Author:
Olivia M. Y. Ngan, CUHK Centre for Bioethics, The Chinese University of Hong Kong, Hong Kong.
Email: oliviangan@cuhk.edu.hk

permits actions with both good and bad effects when 4 conditions are met. The first clause requires that an act performed is not morally evil. Data privacy breaches require direct infringement on one's private zone, sometimes without permission, which does not satisfy the first condition. However, while the act is professionally wrong, there are situations in which doctors regularly break the doctor-patient confidentiality, such as disclosure of HIV status to monitor and stymy the epidemic.[5]

The second clause requires that good effects do not result from evil effects. Under normal circumstances, the government should neither access nor reveal patients' information to uphold confidentiality. Yet, if the government does not release the information of patients infected with the virus, it is possible to cause a more severe community outbreak. With disclosure, other people could avoid virus hotspots and maintain hygiene to prevent communal infection. Some regions controversially disclosed patients' ages, residence, and confirmation date, information which is not disclosed in normal clinical settings.[6,7] Notably, these regions have fared better than their Western counterparts.

However, information disclosure reveals secondary issues—social stigmatization and economic loss. In South Korea, a second outbreak was linked to nightclubs and bars in Seoul's LGBTQ neighborhood.[8] To identify potentially infected individuals, the authorities accessed telecom and credit card information without consent from consumers, and planned to arrange massive testing for over 10,000 identified people who visited affected venues. Many patrons being contacted on home telephone had not revealed sexual orientation to family. The scrutiny on nightlife areas raises concerns about labelling of vulnerable LGBTQ populations, where non-heterosexuality remains taboo in the country. The same is akin to labelling immigrant workers in Singapore as disease spreaders, which further lowers the social status of an already stigmatized group. In Hong Kong, release of specific restaurants usually frequented by blue collar workers involved in the region's third-wave crisis damaged the restaurants' earnings even after thorough cleaning and quarantine measures effectively eliminated risk. Street stalls that cater to lower wage workers, which represent a significant portion of food industry, are seen as less clean than higher-end venues. Naming certain types or venues as disease vectors can entrench class differentiation and dampen economic recovery.

The third clause requires that only good effect is intended. The goal in pandemic is to eradicate diseases and interim collective good is to raise public responsiveness. The *Precautionary Principle* contends that an action is justified when benefits/risks are uncertain. In other words, it is better to be safe than sorry. Among the unknowns with imminent high transmission rate, releasing data as precautionary measure is justified to protect the public from intangible harm until sufficient evidence is accrued.

The fourth clause demands to have proportionate reasons for causing harm, which is in accordance with *Proportionality Principle.* The proportionality to qualify that access to personal data is licit as long as data breach is unintended and no more private information is used than what is necessary. Breaching confidentiality is principally bad and it must employ the least restrictive measures to achieve its goal. For example, only releasing a reasonable amount of sensitive data to achieve good effects. It should be noted that respecting privacy is not an absolute duty[9] and the common good takes precedence over individual right in the pandemic. Response to pandemic requires responsible behavior from community stakeholders. *The Notion of Reciprocity* advocates cooperation between infected patients, uninfected individuals, and social practice to curb virus spread. Eroding privacy, though, is a disproportionate individual burden, big data analytics are conferring non-maleficence and health maximization of the public. The benefit of such actions remains ambiguous, yet the damage to the individual is absolutely not only in this pandemic but also future crises.

There would be fears of misuse when exemptions are made without clear boundaries as to what purpose could or could not be served. For example, if data access could be exempted for public health reasons, is it permissible to serve dragnet surveillance? A Hong Kong territory-wide electronic system often used for public utilities, known as 'Octopus,' provided aggregated anonymous data to stem the local spread. However, whether or not the current users are adequately informed about the data sharing is questionable. Implicit consent, if considered as consent, was exercised, which may have exploited individual autonomy. This istance of breaching privacy for societal purposes is framed by previous uses of electronic transaction systems to track political demonstrators during periods of unrest.[10] Many locals, thereafter, opted out from the system. The success of big data analysis must rely on public participation and trust. Without an open mechanism, erosion of trust has lasting effects, especially in regions with political-social unrest. The government shall then be accountable for data protection, security, and compliance where future instances of data sharing are necessary to acheive public health goals but tarnished by past mishandlings.

These precedent examples highlight that electronic tools initially used for utilities now outlast their purposes to be considered as a monitoring tools. Given that privacy breaches harm the individual but also produce social benefit, there is a proportionate reason to tolerate reasonable, well explained, and accountable privacy infringements in the pandemic to protect community welfare. In the post–coronavirus disease era, heightened levels of surveillance maintained for other purposes require prudent deliberations.

Author Contributions

OMYN conceived and wrote the first draft of the manuscript. OMYN and AK made substantial contribution to the intellectual content and participated in drafting and revising the manuscript. All authors read and approved the final manuscript.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

Ethics Approval

The article is a conceptual discussion and does not require ethics clearance.

ORCID iD

Olivia M. Y. Ngan https://orcid.org/0000-0002-2258-0806

References

1. Lin L, Hou Z. Combat COVID-19 with artificial intelligence and big data. *J Travel Med*. 2020;27:taaa080. doi:10.1093/jtm/taaa080
2. Wang CJ, Ng CY, Brook RH. Response to COVID-19 in Taiwan: big data analytics, new technology, and proactive testing. *JAMA*. 2020;323:1341-1342.
3. Klonowska K, Bindt P. The COVID-19 pandemic: two waves of technological responses in the European Union. Accessed August 14, 2020. www.jstor.org/stable/resrep24004
4. Reeves JJ, Hollandsworth HM, Torriani FJ, et al. Rapid response to COVID-19: health informatics support for outbreak management in an academic health system. *J Am Med Inform Assoc*. 2020;27:853-859.
5. Lin L, Liang BA. HIV and health law: striking the balance between legal mandates and medical ethics. *Virtual Mentor*. 2005;7:687-692.
6. Jung G, Lee H, Kim A, Lee U. Too much information: assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea. *Front Public Health*. 2020;8:305.
7. Centre for Health Protection, Department of Health, The Government of the Hong Kong Special Administrative Region. Coronavirus disease (COVID-19) in Hong Kong. Accessed December 12, 2020. https://www.coronavirus.gov.hk/eng/index.html
8. Kim MH, Cho W, Choi H, Hur JY. Assessing the South Korean model of emergency management during the COVID-19 pandemic. *Asian Stud Rev*. 2020:1-12. doi:10.1080/10357823.2020.1779658
9. Ross D, Ross WD. *The Right and the Good*. Oxford University Press; 2002.
10. Hong Kong protests: police use court orders to obtain protesters' digital fare payment details in another weekend of petrol bombs, tear gas and fires on the streets. Accessed August 14, 2020. https://www.scmp.com/news/hong-kong/politics/article/3029831/hong-kong-protests-police-obtain-court-orders-access