Blog

COVID-19: How public health emergencies have been repurposed as security threats

Shedding light on the capacity of technology to trace and monitor the movement of individuals.

Dr Matthias Wienroth , Dr Gabrielle Samuel , Dr Arely Cruz-Santiago , Dr Jodyn Platt

16 July 2020

Reading time: 17 minutes

The COVID-19 pandemic is shedding light on the capacity of technology to trace and monitor the movement of individuals. This is not new. What is new is the discourse surrounding it, and the potential normalisation of this form of surveillance as a public health imperative. We draw on the concept of biosecuritisation to frame these issues.

Much discussion around COVID-19 public health apps has focused on how to ensure functionality, including on how to measure proximity between phone users and whether apps should adopt a centralised or decentralised approach to the management of data collected.

While these debates are important, the international race to create the 'perfect' technology to contain the transmission of COVID-19 hinders broader discussions on biosecurity and the normalisation of surveillance technologies.

Security experts have warned that digital solutions deployed to control the spread of the virus can, and are, being re-appropriated to introduce and normalise increased, automated and routinised population surveillance for purposes beyond the ones initially intended. While public concern about this has been documented, such developments provide insights on how *public health* emergencies have been repurposed as *security threats*.

The concept of securitisation offers an insightful way to explain this phenomenon.

Sarah Léonard explains that describing phenomena as security threats can enable policymakers and governments to justify actions that would otherwise not be accepted. When an issue is 'securitised', says Léonard,[1] it is presented 'as an existential threat to the survival of a "referent object" (e.g. a state, national identity, etc.) and is accepted as such by the 'audience' of the speech act (e.g. the government, public opinion, etc.).' This, in turn, enables the claim 'that the issue" [requires] emergency measures and [justifies] actions outside the normal bounds of political procedure"'.

And the use of metaphors in the public discourse helps to amplify the sense of a 'security threat'. For instance, the notion of 'fighting COVID-19' and calls to 'stay alert' suggest a war-like, battle-ready situation. In the UK, opinion and decision-makers invoked the 'Dunkirk spirit', when calling on scientists and industry to work together on COVID-19 test and vaccine development. In the US, President Donald Trump, on 23 March 2020, invoked a state of war against an 'invisible enemy'.

While the control of life has always been at the centre of biopower,[2] the term 'biosecuritisation' has recently been applied to describe two generalised approaches to the 'securitisation of life':[3]

1. **a.** to develop *biosecurity regimes* protecting nations against biothreats, e.g. the pre-entry screening of migrants for illnesses such as tuberculosis[4]

   b. to obscure the complex material and discursive work that goes into creating commodities out of biological materials and labour in order to secure social investment into the health and well-being of the nation, e.g. efforts to develop synthetic blood in order to secure a more reliable, safer, and more profitable supply of blood.[5] We could refer to this second approach more widely as economically driven *health security*

Kath Weston places both understandings of the term biosecuritisation within neoliberalism as an example of the 'capitalisation of nature'. Both raise concerns about equity, marginalisation, and abuse of power.

In the current drive towards big data collection and analysis around COVID-19, biosecurity regimes and health security are reflected: public health becomes about both national and economic security. The 'capitalisation of health' is expressed through increasing scientific and computational capacities to analyse and quantify individual data as health data. And the 'datafication of health'[6] builds on notions of commodification[7] and assetisation[8] of health data, patients, and healthcare.

Combining both aspects of biosecuritisation, we can understand fear-driven scenarios post-9/11, that were used to justify increased investment in surveillance technologies in US hospitals, as biosecuritisation.[9] Guided by promises attached to digital technologies as 'technological fixes' to security threats,[10] the rationalisation of healthcare resources was geared towards vendors eager to sell such technologies, and healthcare organisations willing to buy them. This translated into a reduction in funding for other aspects of the healthcare enterprise, such as targeted improvements in medical care.[11]

In the current COVID-19 public health emergency too, we are witnessing how the tropes of biosecuritisation shape the way that the state (Government ministers, advisory groups), the market (businesses, Big Pharma, Google and Apple) and public health bodies (the NHS, NHSX, research groups) attach promises to digital 'track and trace' surveillance as a necessary form of digitally-enabled security.

Biosecurity frameworks invoke 'fear appeals' that are familiar tools in the arsenal of public health.[10] Decades of such tactics have been shown to be ineffective at best, if not unethical, harmful or counterproductive.[13] Fear-based communication may dissuade people who are already skeptical of surveillance, while doing little to change behaviour among people who are already comfortable sharing personal information digitally. There is some preliminary evidence that those nations which use hostile framings of the COVID-19 pandemic are far behind in containing outbreaks, compared to countries that called for unity and collective action.

Features of biosecuritisation also include an emphasis on compliance as a moral imperative.

For instance, on 5 May 2020, UK Health Secretary Matt Hancock proposed that everyone should be 'doing your duty' by using the track and trace app. Later in the month, on 27 May, he framed 'track and trace' in terms of a 'national effort', doubling down morally by linking the uptake of the app to 'civic duty'. By invoking individuals' duty – that is by drawing on a deontological mode of justification for compliance with Government wishes – the Health Secretary was emphasising that, in order to face COVID-19, citizens must submit to this new form of automated surveillance as an obligation in 'good citizenship'.

The moralisation of mobile app usage was even stronger in Australia where, on 17 April 2020, Prime Minister Scott Morrison urged citizens to download the app: 'as a matter of national service'.

Obligation-focused understandings of citizenship go hand-in-hand with a form of conservative governmentality that emphasises individual responsibility towards society over individual rights, e.g. to privacy, including informational self-determination. This notion draws on arguments not dissimilar to the justification of (temporary) curtailment of civil liberties at times of war.

The current COVID-19 pandemic is a public health threat that needs an urgent response. Preparedness is important, and investment in technological surveillance tools is vital if they can be shown to enhance responsiveness to, and perhaps even prevention of public health crises.

However, framing these issues in terms of *biosecuritisation* requires us to critically reflect on the political and moral economy of financial and social investment into technologies such as public health apps.

It also requires us to interrogate the arguments and justifications associated with surveillance technologies, reminding us that the reliability and utility – or more broadly the value, be that ethical, practical, or political – of surveillance technologies cannot be presumed. Values related to technology are socially constructed and as such subject to debate and means of finding agreement.[14]

The NHSX's sudden U-turn on England's digital contact tracing app highlights this.

Metaphors and promissory discourses of a technological fix to a security threat have been used to garner support for, and investment in the app. When the Isle of Wight trial exposed issues with the technologies' reliability and utility (something that a comprehensive, multi-perspective, critical assessment of the discourse would have identified, e.g. via findings on the limited utility of Bluetooth as a means of reliably measuring distance)[15] the biosecuritisation discourse had to change. And so the UK Government reframed the situation as 'the next phase' to fit its U-turn into their narrative.

The current biosecuritisation framing requires us to reflect on the fact that the digital industry's promises of enhancing security and containment of COVID-19 are likely more related to their commercial and data interests than to any evidence that their technologies can achieve this.

monitoring populations.

These considerations must be situated – as does much of the COVID-19 response in the UK – within the context of the capitalisation of health, including health data. This includes the fostering of life sciences research via large population data drives, the dismantling of the National Health Service as a state enterprise in favour of a competitive health market, and the increased sharing of healthcare and health data with commercial providers.[16]

During their response to COVID-19, NHSX, the technology arm of the UK's National Health Service (NHS), has drawn on advice from a range of technology companies, including on Mustafa Suleyman, Google executive and DeepMind co-founder, who oversaw the NHS data sharing project, on how to collect confidential patient information.

Lack of critical engagement with biosecuritisation discourses can lead to normalisation, entrenchment and dominance of certain modes and logics of surveillance that would have been thought unfeasible and unjustifiable until recently. For instance, the Israeli cyber intelligence firm NSO Group has historically only provided services to government authorities in order to tackle terrorism and crime, but is now marketing a software that uses mobile phone data to detect and predict the spread of COVID-19.[17] NSO Group is facing legal action due to its software being used on mobile phones to pry on journalists, human rights defenders and advocacy workers from Mexico to the Middle East; including high profile cases, such as the assassination of Jamal Khashoggi inside the Saudi consulate in Istanbul.

It is not unthinkable that the conflation of these two types of data generation may be intentional, with potentially wide-reaching curtailment of personal freedoms and civil liberties through dual app/data use.

In conclusion, we are not saying that the legitimacy of specific technologies and their use cannot, or must not, change in certain circumstances. They do and sometimes even need to. The introduction into practice of technologies with significant potential to change the rights and obligations of citizens, however, as in the case of contact tracing apps, must always be accompanied by a broad and transparent societal debate that is not afraid to critically scrutinise and challenge dominant narratives, including the framing of public health emergencies as security threats.

The authors would like to thank Chris Lawless (Durham University) and Ernesto Schwartz-Marin (University of Exeter) for discussions on securitization and dual use in the case of the COVID-19 contact tracing app.

Dr Samuel's work on COVID-19 tracing apps is funded by a Wellcome Trust grant: 213619/Z/18/Z/.

Dr Cruz-Santiago's work on data justice and multiveillance is funded by an ESRC grant: ES/R009945/1.

References

Ada Lovelace Institute. "Exit through the app store: how the UK Government should use technology to transition from the COVID-19 global public health crisis." Ada Lovelace Institute Blog, April 20, 2020.

BBC News (2020) "Jamal Khashoggi: all you need to know about Saudi journalist's death." *BBC*, July 2, 2020.

Birch, K. (2017). "Rethinking value in the bio-economy: finance, assetization, and the management of value." *Science, Technology, & Human Values,*42(3), 460-490.

Boseley, S. and Stewart, H. "Hancock: it is public's 'civic duty' to follow test-and-trace instructions in England" *Guardian,* May 27, 2020.

Chapman S. (2018). "Is it unethical to use fear in public health campaigns?" *American Journal of Public Health*, 108(9), 1120-2.

Cho H, Salmon C.T. (2006). "Fear appeals for individuals in different stages of change: intended and unintended effects and implications on public health campaigns." *Health communication*, 1;20(1), 91-9.

Cruz- Santiago, A.(Forthcoming). "Normalising Digital Surveillance: Data Justice Amidst Covid19." Taylor, L; Sharma, G; Martin A.K; Jameson, S.M. (eds). *Data Justice and Covid19: Global Perspectives*. London: Meatspace Press.

Davenport, S., Kunicova J. and Kallaur, E. "We're all in this together: collective action and trust in the age of coronavirus." *World Bank Blogs*, April 20, 2020.

Department of Health and Social Care. "Next phase of NHS coronavirus (COVID-19) app announced." Gov.uk, June 18, 2020.

Dheensa, S., Samuel, G., Lucassen, A. M., & Farsides, B. (2018). "Towards a national genomics medicine service: the challenges facing clinical-research hybrid practices and the case of the 100 000 genomes project." *Journal of Medical Ethics*, 44(6), 397-403.

Fisher, J.A. and Monahan, T. "The 'biosecruization' of healthcare delivery: examples of post 9/11." *Social Science and Medicine*, 72(4), 545-552.

Foucault, M. (2007). *Security, territory, population. Lectures at the College of France*. Palgrave Macmillan.

Francis Crick Institute (2020) "Francis Crick Institute and UCLH develop COVID-19 testing service for patients and NHS staff." April 2, 2020.

Gould, M., Joshi, I. and Tank M. "The power of data in a pandemic." uk, March 28, 2020.

Guardian (2020) "'Invisible enemy': Trump says he is "wartime president" in coronavirus battle-video." Guardian, March 23th, 2020.

Guttman N, Salmon C.T. (2004). "Guilt, fear, stigma and knowledge gaps: ethical issues in public health communication interventions." *Bioethics*, 18(6), 531-52.

Henderson, S., and Petersen, A. R. (eds.) (2002). *Consuming health: the commodification of health care*. Psychology Press.

Holmes, Oliver, Justin McCurry and Michael Safi. "Coronavirus mass surveillance could here to stay, experts say." *Guardian,* June 18, 2020.

Johnston, J. "Matt Hancock says public has a 'duty' to download coronavirus contact tracing app." *PoliticsHome*, May 5, 2020.

Kaunert, C. and Léonard, S. (eds) (2012). *Developing European internal security policy. After the Stockholm Summit and the Lisbon Treaty*. London: Routledge.

Kavanagh, C. (2019). "New tech, new threat and new governance challenges: an opportunity to craft smarter responses." Carnagie Endowment for International Peace.

Kaye, B and Packam C. "Australians urged to adopt phone tracking app in coronavirus fight." *Reuters, April 17, 2020.*

Kitchin, R. (2020). "Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19." *Space and Polity*, DOI:10.1080/13562576.2020.1770587.

Klein, N. "Naomi Klein: how big tech plans to profut from the pandemic." *Guardian,* May 13, 2020.

Leith, D.J. & Farrell, S. (2020). "Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection." Dublin: Trinity College. 6 May 2020.

Murphy, M. (2020) 'Google executive advised NHS on how to collect confidential patient data' *The Telegraph.* 1 June 2020.

Papadopoulos, D. (2015). "From publics to practitioners: invention power and open technoscience." *Science as Culture*, 24(1), 108-121, DOI: 1080/09505431.2014.986322

Rose, H. (2001). *The commodification of bioinformation: the Icelandic health sector database*. London: Wellcome Trust.

Ruckenstein, M., & Schüll, N. D. (2017). "The datafication of health." *Annual Review of Anthropology*. 46, 261-278.

Shah, Sooraj. "Consumers worry that COVID-19 contact tracing data will be used for other purposes. Here is why." *Forbes,* June 24, 2020.

Skinner, D., & Wienroth, M. (2019). "Was this an ending? The destruction of samples and deletion of records from the UK police national DNA database." *BJHS Themes*, *4*, 99-121.

Warren, A. (2013). "(Re)locating the border: Pre-entry tuberculosis (TB) screening of migrants to the UK." *Geoforum,* 48, 156-164,

Weston, K. (2013). "Biosecuritization: The quest for synthetic blood and the taming of kinship." Johnson, C. H., Jussen B., Warren Sabean D. and Teuscher S. (eds.) *Blood and kinship. matter for metaphor from ancient Rome to the present.* Berghahn Books, 244-265.

Wienroth, M. and Lipphardt, V. (2017) "Wissenschafte, ethisce & soziale Gesichtspunkte der Anwendung neuer Gen-Analysen im polizeilichen Ermittlyngsdienst." 21 Marz 2020.

Wienroth, M., Pearce, C. and McKevitt, C. (2019). "Research campaigns in the UK National Health Service: patient recruitment and questions of valuation." *Sociology of Health & Illness*, 41(7), 1444-1461.

Footnotes

1. Kaunert and Léonard, Developing European Internal Security Policy. After the Stockholm Summit and the Lisbon Treaty, p. 93. ↑

2. E.g. Paul Nurse, Director of the Francis Crick Institute, on 2 April 2020: https://www.crick.ac.uk/news/2020-04-02_francis-crick-institute-and-uclh-develop-covid-19-testing-

3. Foucault, Security, Territory, Population. Lectures at the College of France, pp. 436. ↑

4. Papadopoulos "From Publics to Practitioners: Invention Power and Open Technoscience". ↑

5. Warren, "(Re)locating the border: Pre-entry tuberculosis (TB) screening of migrants to the UK". ↑

6. Weston, "Biosecuritization: The quest for synthetic blood and the taming of kinship", p. 247. ↑

7. Ruckenstein and Schüll, "The datafication of health". ↑

8. Henderson and Petersen, Consuming health: The commodification of health care; Rose, The commodification of bioinformation: The Icelandic health sector database. ↑

9. Birch, "Rethinking value in the bio-economy: Finance, assetization, and the management of value"; Wienroth, Pearce, and McKevitt, "Research campaigns in the UK National Health Service: patient recruitment and questions of valuation". ↑

10. Fisher and Monahan, "The 'biosecruization' of healthcare delivery: examples of post 9/11". ↑

11. E.g. Kavanagh, "New tech, new threat and new governance challenges: an opportunity to craft smarter responses."; Kitchin, "Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19". ↑

12. Fisher and Monahan, "The 'biosecruization' of healthcare delivery: examples of post 9/11". ↑

13. Chapman, "Is It Unethical to Use Fear in Public Health Campaigns?"; Cho and Salmon, "Fear appeals for individuals in different stages of change: intended and unintended effects and implications on public health campaigns"; Guttman and Salmon, "Guilt, fear, stigma and knowledge gaps: ethical issues in public health communication interventions". ↑

14. Cf. Wienroth and Lipphardt, "Wissenschafte, ethisce & soziale Gesichtspunkte der Anwendung neuer Gen-Analysen im polizeilichen Ermittlyngsdienst"; Skinner and Wienroth, "Was this an ending? The destruction of samples and deletion of records from the UK police national DNA database". ↑

15. Leith and Farrell, "Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection". ↑

16. Dheensa, Samuel, Lucassen, and Farsides, "Towards a national genomics medicine service: the challenges facing clinical-research hybrid practices and the case of the 100 000 genomes project". ↑

17. Cruz- Santiago, "Normalising Digital Surveillance: Data Justice Amidst Covid19". ↑

Additional download	Exit through the App Store? Rapid evidence review (PDF 864 KB) ↓
Programme	Health data and COVID-19 tech
Keyword	Contact tracing
Authors	Dr Matthias Wienroth · Dr Gabrielle Samuel · Dr Arely Cruz-Santiago · Dr Jodyn Platt