Our Digital Footprint under Covid-19: Should We Fear the UK Digital Contact Tracing App?

Audrey Guinchard, Senior Lecturer, School of Law, University of Essex [DOI: 10.5526/xgeg-xs42_034]

Abstract

With the objective of controlling the spread of the coronavirus, the UK has decided to create and, since 5 May 2020, is live testing a digital contact tracing app, under the direction of NHS X, a branch of NHS Digital, and with the help of the private sector. Given the lack of details as to what the app will exactly do or not do, there are fears that the project will increase government surveillance beyond the pandemic. While I share these concerns, I argue that we need to simultaneously tackle one of the most significant, yet overlooked, contributors to the problem of government surveillance: our inflated digital footprint, stemming from our use of digital technology, and the basis of 'surveillance capitalism', a business model left largely unchallenged, which results in surveillance, and stems from the non-compliance with data protection laws. A systematic enforcement of the General Data Protection Regulation (GDPR) on the private sector would disrupt the current dynamics of surveillance which are hidden in plain sight.

I. Introduction

Confronted with the Covid-19 public health crisis, more than 30 countries have already instituted measures to track people's movements, with the objective of controlling the spread of the virus and/or people's movement.[1] Mobile phone apps are central to these efforts.[2] The UK has decided to create and, since 5 May 2020, is live testing a digital contact tracing app, under the direction of NHS X, a branch of NHS Digital, and with the help of the private sector. The app has so far attracted a number of concerns, correlative recommendations,[3] and a draft Bill.[4] Given the lack of details as to what the app will do, fears exist that the project will create a huge data trove, without adequate safeguards, in violation of data protection laws and human rights, and with the potential to open the door to extensive government surveillance beyond the management of the current public health crisis.

I share those concerns and agree with the various recommendations put forward but I argue that we need to simultaneously tackle one of the most significant, yet overlooked,

[1] Andrew Roth and others, 'Growth in surveillance may be hard to scale back after pandemic, experts say' The Guardian, 14 April 2020.
[2] Ada Lovelace Institute, 'Exit through the App Store? A rapid evidence review on the technical considerations and societal implications of using technology to transition from the COVID-19 crisis,' 20 April 2020.
[3] Ibid.; academics in: Rachel Coldicutt, 'Open Letter: Contact Tracking and NHSX,' *Medium*, 23 March 2020; Matthew Ryder QC et al., 'COVID-19 & Tech responses: Legal opinion,' 30 April 2020; House of Commons Science and Technoogy Committee, 'Oral evidence: UK Science, Research and Technology Capability and Influence in Global Disease Outbreaks', HC 136, Questions 302-384, 28 April 2020; Joint Committee on Human Rights (JCHR), 'Human Rights and the Government's Response to Covid-19: Digital Contact Tracing', 6 May 2020.
[4] Initially, an academic initiative, Lilian Edwards et al., 'The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates. Version 5.1,' 6 May 2020, https://osf.io/preprints/lawarxiv/yc6xu/; now a proposal put forward by the JCHR, 'Committee drafts Bill on Covid-19 (Coronavirus) Contact Tracing App', 15 May 2020.

contributors to the problem of government surveillance: our inflated digital footprint, the basis of 'informational capitalism' or 'surveillance capitalism', a set of surveillance practices elevated to a business model and left largely unchallenged.[5] To do so requires the systematic enforcement of the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 on the private sector so as to disrupt the current dynamics of surveillance which are hidden in plain sight.

After a brief outline of the data protection law framework applicable to the processing of personal data in general, I will sketch the main elements of the controversy surrounding the app before explaining its context, i.e. the surveillance business model that part of the private sector has adopted, in violation of data protection laws. I will thereafter highlight the resulting dynamics and why they need challenging, concluding that enforcement by the UK data protection regulator, the Information Commissioner Office (ICO) should play a central role in altering these dynamics, beyond the Covid-19 crisis.

II. The Backdrop: The Data Protection Law Framework

The GDPR, like the Directive 1995/46/EC it replaced on 25 May 2018, established a number of legal requirements for the processing of persona data. The principles are the necessity (not just convenience of processing) and proportionality of the processing as to the types of data collected, the purposes for which they are used, the time during which they are needed for processing, and the legal grounds to justify the processing.[6] Controllers, who decide the purposes and means of processing, should ensure compliance with the above principles and demonstrate compliance. Processors acting on behalf of controllers have, since the GDPR, a much more pro-active role in ensuring compliance, with specific duties, independently of controllers' own obligations (Article 28 GDPR).

Compliance with data protection laws is not a tick-box exercise to be undertaken after the digital technology has been created. In case of high risk processing, such as health data processing, data protection impact assessments have become mandatory, so as to mitigate risks, and if mitigation is not possible, to decide whether the processing should be pursued at all.[7] Compliance with human rights is also central to data protection by design.[8] Indeed, the ultimate objective of all these rules, in the GDPR (Recital 4) and in the Directive (Recital 2), is that 'the processing of personal data should be designed to serve mankind'. The controversy surrounding the digital contact tracing app centres around these sets of obligations.

III. The Controversy Surrounding the UK Digital Contact Tracing App

NHS X leads the development of the app, with the help of the private sector. It thus determines the purpose and means of processing, and as a data controller, needs to ensure compliance with the key principles. The companies it works with are likely to be considered as processors, acting on behalf of NHS X which should instruct them to

[5] Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (New York: Oxford University Press, 2019); Shoshana Zuboff, *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power* (London: Profile Books, 2019).
[6] Articles 5 and 6 GDPR, very similar to Articles 6 and 7 Directive.
[7] Article 35 GDPR.
[8] Recital 4 GDPR; the ICO Elizabeth Denham, JCHR, 'Oral evidence (virtual proceeding): The Government's response to Covid-19: human rights implications', HC 265, Questions 10-14, 4 May 2020.

implement data protection by design. The little information NHS X has so far provided has remained scattered and vague.[9] The app processes Bluetooth data to be stored in a 'backend datastore' and aggregated with some data sets, such as the Covid-19 test results and the details of the 111 call,[10] but without further details beyond the potential or likelihood of adding geolocation data in a future iteration of the app.[11] This centralised approach allows creating a social graph of individuals' and their interactions with others to understand the spread of the disease and hot spots of infections. Hence doubts as to implementing data minimisation. Furthermore, the exact purposes for which the data will be used have not been explained, beyond a vague reference to tracing and research, raising issues as to compliance with the purpose limitation. Time limitation is also a problem since the Bluetooth data, 'enmeshed with wider data', cannot be deleted.[12]

Regarding the legal grounds to justify processing, NHS X has continuously indicated that consent will be sought, presenting consent as an indicator of its commitment to privacy and the law.[13] It is however extremely unlikely that consent can justify the processing, especially for research, in light of the long standing EU guidance on data protection consent,[14] specifically repeated for Covid-19 tracing apps.[15] NHS X seems to confuse the voluntary nature of using the app with the legal justification for processing data, despite the ICO having expressly pointed out the difference.[16] This betrays wider issues as to the understanding of the law and the nature of the conversations with the ICO.

To reassure critics, NHS X has finally opened the source code of the app, but not of the datastore,[17] and published the data protection impact assessment (DPIA),[18] voluntarily submitted the DPIA to the ICO.[19] Nevertheless, since 'the devil is in the details',[20] especially with regard to the datastore, suspicions as to the UK government's surveillance capability have not abated. In fact, the JCHR appears to be alarmed by the speed of the piloting and intended roll out.[21] Data protection by design requires to pause and ascertain those risks *before* the app is rolled out, not afterwards.

---

[9] Only two official statements -of 28 March and 28 April 2020-, with information added when Matthew Gould, head of NHS X, testified before the House of Commons Science and Technology Committee on 28 April 2020, and the JCHR on 4 May 2020.
[10] Matthew Gould, Indra Joshi, and Ming Tang, 'The power of data in a pandemic,' 28 March 2020, https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/.
[11] House of Commons Science and Technoogy Committee (n. 3), Q340, 376.
[12] Matthew Gould, Q20, JCHR, 'Oral evidence (virtual proceeding): The Government's response to Covid-19: human rights implications', HC 265, Questions 10-14.
[13] House of Commons Science and Technoogy Committee (n. 3), Q 326, 340, 341, 364, 366; JCHR, 'Oral evidence (virtual proceeding): The Government's response to Covid-19: human rights implications', HC 265, Q17.
[14] Article 29 Working Party, 'Guidelines on consent under Regulation 2016/679. WP 259 rev.01,' 2018. Now replaced by EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.0,' 4 May 2020.
[15] EDPB, 'Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak,' 16 March 2020.
[16] ICO, 'COVID-19 Contact tracing: data protection expectations on app development,' 4 May 2020.
[17] 'Source code of the digital contact tracing Covid-19 app,' Github, 7 May 2020, https://github.com/nhsx.
[18] DPIA.
[19] ICO, 'Statement in response to media enquiries about the Data Protection Impact Assessment for the NHSX's trial of contact tracing app', https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/dpia-for-the-nhsx-s-trial-of-contact-tracing-app.
[20] Prof Lilian Edwards, House of Commons Science and Technoogy Committee (n. 4), Q362.
[21] JCHR, 'Human Rights and the Government's Response to Covid-19' (n. 3), 12; JCHR, 'Oral evidence (virtual proceeding): The Government's response to Covid-19: human rights implications', HC 265, Q 17.

So far, recommendations have centred on restricting government's abuse of power. I argue that this approach will not suffice. Once we start looking at the digital contact app from the perspective of the digital ecosystem and our massive digital footprint,[22] the app can hardly be seen as 'something new because this degree of surveillance of members of the public has never been contemplated before'.[23]

IV. Contextualising the Controversy: A Business Model Resulting in Surveillance

Our society tolerates commercial practices that result in massive and intrusive surveillance, which if they had originated from governments, we would be, I submit, up in arms. Because they come from the private sector and are more diffused, lost in an ecosystem so opaque that we do not know exactly what our digital footprint consists of and who has access to it,[24] we have not opposed them. Let us look at Bluetooth which the digital contact app will use. Bluetooth has been invented for connecting two devices, for example a pen to a tablet. Bluetooth's use was transformed when Apple created in 2013 the iBeacon for apps to micro-target consumers in stores.[25] Bluetooth is now ubiquitous in airports, hotels, and shops to 'customise their experience', an euphemism that masks the tracking of their movements.[26] Thus, while Bluetooth has undeniable benefits, it also has an inherent capacity for surveillance.

Now, let us imagine the following Covid-19 scenario. The lockdown has eased, an employer interviews three different individuals, hiding from each a smartphone with the app on.[27] Each interviewee has the app; one tests positive for Covid-19; the interviewer receives notification. Will the interviewer decide that hiring the interviewee is not worth the risk, or on the contrary, in the (false?) belief that herd immunity can be built on, will it favour the interviewee who had Covid-19, as employers and slave owners used to do for those who contracted the yellow fever in 19th century New Orleans?[28] Whichever decision the modern employer will take, how will the interviewees know whether the positive testing for Covid-19 influenced the decision? The current debate on the Covid-19 digital contact tracing app has not really pointed out this inherent risk of misuse, independently of whether a decentralised or centralised approach is adopted.

More generally, given the wide use of Bluetooth in the private sector, where are the studies on the resulting surveillance? If iBeacon had been invented by a governmental intelligence agency, would our reaction have been different? Surveillance in Western countries is still

---

[22] David L. Chaum, 'Security without identification: transaction systems to make big brother obsolete,' *Commun. Assoc. Computing Machinery* 28, no. 10 (1985). The author, at the origins of key elements of cryptography and the dark web, is cited in the PEPP-PT project, which is somewhat ironic given the criticisms of surveillance for the PEPP-PT project, PEPP-PT (n. 39).

[23] Joanna Cherry, considering the app as something new, Member of the JCHR, 'Oral evidence (virtual proceeding): The Government's response to Covid-19: human rights implications,' HC 265, Q4 p10.

[24] See the work of ICSI—UC Berkeley and IMDEA Networks, "The Haystack Project," 21 February 2020, https://www.haystack.mobi.

[25] Michael Kwet, 'In Stores, Secret Bluetooth Surveillance Tracks Your Every Move' *New York Times*, 14 June 2019. Nic Newman. Apple iBeacon technology briefing. J Direct Data Digit Mark Pract 15, 222–225 (2014).

[26] Ibid.

[27] The scenario is not mine, see (in French) Xavier Bonnetain, 'Le traçage anonyme, dangereux oxymore. Analyse de risques à destination des non-spécialistes (website),' 23 April 2020 , https://risques-tracage.fr.

[28] Kathryn Olivarius, 'Immunity, Capital, and Power in Antebellum New Orleans', (2019) 124 The American Historical Review 425.

associated with state agencies, but they do not need anymore to directly collect data when they have an enormous readily available pool of data collected by others … in the private sector. When in 2013, Snowden revealed the PRISM programme, it became clear that the NSA focused on building its capacity to *aggregate* and *analyse* the data, relying on US private companies to give the data.[29]

We live in a digital ecosystem where many of the innovative digital technologies we use have been developed in direct opposition to the core legal principles of data protection by design. Instead of minimising processing to what is needed to provide a service, a number of businesses have thrived on collecting as much data as possible from consumers, often under the disguise of 'free services', and by buying and selling the resulting profiling to data brokers. The context directly related to the Covid-19 digital contract tracing apps is particularly representative of this business model's approach to data protection and the risks it creates. Apps on smartphones, fitbits, smartwatches, now abound that collect various health information: the number of steps per day, the speed of the walk/run, weight, height, BMI, and/or various medical health information the user can enter. Many of these health apps violate the GDPR by collecting far too much data, for too long, without transparency, and without securing the data.[30]

As a result, the private sector has access to a granularity of information that can be shocking. Nowadays, an insurer -who acquires supposedly anonymised data from a supermarket loyalty scheme to feed into its predictive algorithm- can identify a client who buys fennel as a healthy conscious consumer who is unlikely to be of high risk, and who thus should be offered a lower premium.[31] Fennel in the UK is a luxury vegetable that not all supermarkets will sell. Most people from deprived areas cannot afford it. 'Given the correlation between unhealthy lifestyles and lower incomes, the risks are only too clear' of discrimination and of further entrenching the inequalities of our society. [32] Yet, the impact on human rights and on the social fabric of our society is barely understood. Over time, the surveillance resulting from this business model is proving to be no less dangerous to human rights than those of governments.

In light of this context, the concerns as to government surveillance through the building of the digital contact tracing app take a different resonance. Undoubtedly, we should ensure that it does not happen, and the safest way to do so is to entrench safeguards in primary legislation. Nevertheless, we should be equally concerned about the possible actions from the private sector and the dynamics that they contribute to. Transparency and accountability should be demanded not just of government, specifically here NHS X, but also of the private sector involved in the project. This discussion has largely been missing, despite data protection laws constituting an excellent starting point to challenge the current dynamics of the project.

---

[29] Glenn Greenwald and Ewen MacAskill, 'NSA Prism program taps in to user data of Apple, Google and others,' *The Guardian*, 7 June 2013.
[30] As the Belgian Data Protection Authority stated on 31 March 2020, https://www.autoriteprotectiondonnees.be/le-covid-19-et-lutilisation-dapplications-de-sante; Norway Consumer Council, "Report: Out of Control", 14 January 2020, https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/report-out-of-control/.
[31] Hannah Fry, 'Hello World: How to be Human in the Age of the Machine', Doubleday, 2018, and interview at https://www.noted.co.nz/tech/tech-tech/how-algorithms-can-go-rogue-whos-at-the-wheel.
[32] Editorial, 'The Guardian view on big data and insurance: knowing too much,' *The Guardian*, 27 September 2018.

V. Revisiting the Controversy: The Need to Challenge the Dynamics of the Digital Contact Tracing App Project

NHS X indicated it works notably (but not exclusively) with Microsoft, Google, Palantir, Amazon Web Services and Faculty AI.[33] Because the government does not have the in-house expertise to build these apps, that it resorted to the private sector should not surprise. This collaboration however needs to respect the rules set out in the GDPR, notably Article 28 GDPR. Controllers have to choose processors who can demonstrate compliance with data protection by design (Article 28(1) GDPR); if the processors' track record does not give full confidence, controllers can refuse to choose them.[34] Furthermore, processors have the duty to assist controllers in fulfilling their obligations, with an expectation to be pro-active (Article 28(3) GDPR). The problem is that NHS X has chosen companies whose implementation of the GDPR has been recently challenged either formally, by a data protection regulator, or informally by academic scientists.

Google has been found twice in breach of data protection laws; [35] and a complaint for its use of a tracking ID on Android has just been filed before the Austrian Data Protection Authority.[36] While Microsoft has a very different business model from Google's, in November 2018, the Dutch Government concluded that its processing of personal data for a wide range of its products[37] violated the GDPR core principles (data, purpose and time limitations). The EU regulator reached the same conclusions in its preliminary investigation.[38] Has the impact of these findings of non-compliance been assessed on the UK contracts in general and on the development of the Covid-19 app in particular? Furthermore, in May 2019, Palantir, which business model is based on buying and selling huge troves of (personal) data,[39] was criticised for selling to the US immigration agency tracking software that enables the agency to take decisions in breach of human rights.[40]

Consequently, doubts as to whether NHS X has complied with Article 28(1) GDPR arise. That NHS X could not confirm, a week before the restricted launch of the app, that Apple and Google would be forbidden to turn off the app at any point, despite having the power to delete the app from their stores, does not give full confidence that NHS X has ensured

[33] Gould, Joshi, and Tang (n. 10). House of Commons Science and Technoogy Committee (n. 3), Q302-384.
[34] EDPS, 'EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725.'
[35] (in English) CNIL, 'Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC.,' 21 January 2019, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc, paras. 105, 109.
[36] By the NGO NYOB, 13 May 2020, https://noyb.eu/en/complaint-filed-against-google-tracking-id.
[37] A summary by those who audited the firm is available at Privacy Company, 'New DPIA on Microsoft Office and Windows software: still privacy risks remaining (long blog),' 29 July 2019, https://www.privacycompany.eu/blogpost-en/new-dpia-on-microsoft-office-and-windows-software-still-privacy-risks-remaining-long-blog. For the full reports: https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise.
[38] Upon referral, EDPB, 'EDPS investigation into IT contracts: stronger cooperation to better protect rights of all individuals,' 21 October 2019.
[39] Peter Waldman, Lizette Chapman, and Jordan Robertson, 'Peter Thiel's data-mining company is using War on Terror tools to track American citizens. The scary thing? Palantir is desperate for new customers,' *Bloomsberg Business Week*, 19 April 2018.
[40] Marisa Franco, 'Palantir has no place at Berkeley: they help tear immigrant families apart,' *The Guardian*, 31 May 2019.

that the companies only act on its instructions.[41] Similarly, if the companies hired are not already fully compliant, doubts exist as to whether they are in a position, for example, to point out to the controller that its instruction may violate the GDPR (Article 28(3) GDPR). Has any of companies for example challenge NHS X's use of consent, when the GDPR violation is likely? Willingness to 'get it right',[42] while laudable, may well not suffice if the structures for compliance are inadequate. Trust in the project cannot rest on the hope that things will turn out all right, especially at a time of crisis.

To summarise, when each partner of a project experiences their own difficulties in complying with data protection laws, their collaboration has the potential to multiply the risks of non-compliance and human rights violations. The GDPR provides the tools to challenge these dynamics.[43] Difficult questions can be asked, but the answers do not have to be provided to the general public. It falls therefore on the data protection regulator, in the UK the ICO, to question decisions that potentially violate the GDPR. So far the Judicial Committee on Human Rights has not been impressed by the ICO's approach to the NHS X's project. [44] More importantly maybe, the Committee had already noted in 2019 a wider trend of not enforcing data protection laws with sufficient vigour. Hence the Committee's recommendation for the Government to review 'whether there are adequate measures in place to enforce the GDPR and DPA in relation to how internet companies are using personal data, including consideration of whether the ICO has the resources necessary to act as an effective regulator.'[45] In May 2020, the recommendation is to create a specific monitoring body for real-time auditing. In the long term, is this a viable solution? Lack of enforcement leaves a vacuum, where others are forced to take decisions which are not within their role[46] and which they do not want to take.[47] It would be more beneficial to strengthen the ICO's capacity to enforce, not the least by internally separating its roles of advisor, investigator and decision-maker, as the Financial Conduct Authority does, to avoid inherent conflicts of interests.[48]

VI. Conclusion

The pandemic has revived fears of governments creating or extending massive surveillance programmes under the cover of fighting the coronavirus and exiting the lockdown. I have demonstrated that the NHS X project suffers from enough flaws with regard to data protection laws to give substance to these fears: a lack of transparency, the recurring vagueness of the little information provided, and the choices made regarding the processors when their compliance with data protection laws can be patchy.

---

[41] House of Commons Science and Technoogy Committee (n. 3), Q 358, 383 – it is commendable though to ask for time to check the answer.
[42] Matthew Gould, JCHR, "Oral evidence" (n. 12), Q18.
[43] But it will not resolve some issues of data sharing facilitated by other legislations, as correctly pointed out by Michael Veale, JCHR, 'Oral evidence (virtual proceeding): The Government's response to Covid-19: human rights implications,' HC 265, Q13.
[44] JCHR, 'Oral evidence (virtual proceeding): The Government's response to Covid-19: human rights implications,' HC 265, Q17.
[45] Ibid.
[46] Ada Lovelace Institute, 'Exit through the App Store' (n. 2) 10.
[47] Microsoft called for regulation of facial recognition, Joseph Menn, 'Microsoft turned down facial-recognition sales on human rights concerns,' *UK Reuters*, 17 April 2019.
[48] The ICO did not see the conflict, JCHR, 'Oral evidence (virtual proceeding): The Government's response to Covid-19: human rights implications,' HC 265, Q17.

Nevertheless, these fears should not mask that part of the private sector indulges into building our digital footprint and use it to extensively monitor us, independently of what governments do. Fitbits and health apps on smartphones are the latest expression of a business model based on little to no compliance with data protection laws. It should be of no surprise then that these businesses pay lip service to privacy rights and to the broader range of human rights which the technology may or will interfere with. In that sense, governments' surveillance could be seen as the last step of a process that has started in part of the private sector. If neither side has an internal culture of compliance, how can they be expected to take responsibility to ensure all safeguards are in place?

To their discharge, the poor enforcement of data protection laws has not contributed to foster a strong culture of compliance with data protection laws. Time has come for a systematic enforcement of the GDPR, which would ultimately bear fruits beyond the decisions taken on specific controllers and processors. The minimisation of processing, and thus of our digital footprint, would become an entrenched habit for all technology developers, with the ripple effect that any deviation would stand out and be easier to challenge. Convenience and functionality of digital technologies do not have to trump the necessary standards of security, privacy, and human rights. It is time to create an environment where developers are rewarded for designs that 'serve mankind' rather than for those that serve short term interests destructive of the fabric of our society.