Some contrarian thoughts on the deployment of contact-tracing apps

These thoughts have been prepared in response to the overwhelming reliance on the advice of a small number of data protection law and privacy experts regarding the deployment of contact-tracing apps. As the balance of this article will argue, the most effective privacy protection framework is the use of ***legal code*** *(The EU Charter of Fundamental Rights/European Convention Of Human Rights and the General Data Protection Regulation (GDPR), etc.), and not* ***software code****. The most appropriate way to ensure privacy protection is through the operation of law.*[1] *This article also argues that not only should governments be held to account for their response to the pandemic, the academic community should also review and reflect on how privacy advocates led the response to a public health emergency.*

In line with developments within the European Union[2]*, this analysis is based on the following presumptions:*

- *Any contact-tracing app will be downloaded by users on a voluntary basis;*
- *No central authority will be permitted to check for compliance and/or enforce the notifications sent to users that recommend that they isolate or get tested*

Contact-tracing apps have emerged as a partial response to slowing down the spread of a highly contagious virus that kills people, especially the most vulnerable members of society. Furthermore, the spread of Covid-19 has been recognized as a major public health emergency.[3] A 'test, track and trace' strategy has been deemed a fundamental part of the process for reopening national economies and the borders of many European countries. The privacy-preserving movement[4] has dominated the way we think about how best to respond to the public health crisis brought on by the spread of COVID-19.

In line with its long-standing commitments to democracy and fundamental rights, various member states of the EU and the United Kingdom are counting on its citizens to act responsibly, download the app, and voluntarily abide by any notifications. While it is true that citizens are not necessarily to be trusted to do this, neither are governments and big tech to be trusted to preserve privacy and not abuse the privilege of access to sensitive health data. The debate has led to irreconcilable differences in approach. If a contact-tracing app is to be downloaded on a purely voluntary basis, the addition of enforcement measures backed up by penalties for failure to comply with notifications to self-quarantine may result in citizens refusing to download the app at all. If downloading the app is made compulsory, this would raise problems with regard to whether such an imposition is incompatible with living in a free society.

This debate raises important empirical questions: Does putting privacy above functionality and effectiveness compromise the effectiveness of our responses? Did the way privacy was protected lead to the most effective results? And pragmatic questions: Is owning a smartphone to be made compulsory? Would you not be allowed to leave your home unless you have a phone with the app running? Would you be denied access to public services (such as transport)?

---

[1] Professor Lilian Edwards's proposal for a draft law to safeguard rights and freedoms is a good example of this, at https://osf.io/preprints/lawarxiv/vc6xu/, (visited 20 May 2020); See also the Human Rights Committee Bill at https://publications.parliament.uk/pa/jt5801/jtselect/jtrights/correspondence/Letter-to-Rt-Hon-Matt-Hancock-MP-Secretary-of-State-for-HSC-Draft-Bill.pdf, (visited 20 May 2020).

[2] European Commission, 'Coronavirus: Commission adopts Recommendation to support exit strategies through mobile data and apps', at https://ec.europa.eu/commission/presscorner/detail/en/ip_20_626, (visited 17 May 2020).

[3] The outbreak was declared a Public Health Emergency of International Concern on 30 January 2020 at https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen

[4] Pan-European Privacy-Preserving Proximity Tracing at PEPP-PT: HOME; See also PEPP-PT vs DP-3T: The coronavirus contact tracing privacy debate kicks up another gear: "On one side of the divide is a consortium of academics and business stakeholders converging under the PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) umbrella"

But it also raises questions about the role of privacy advocacy itself. Just how was the privacy-preserving movement able to dominate the discussion in the first place? Often overlooked in this debate is the fact that the state has a positive obligation to protect the lives of its citizens[5], as well as their 'physical and mental integrity'[6]. Importantly Article 52 of the EU Charter states that 'respecting the essence' of rights like the right to life, privacy, and data protection cannot be compromised even when those rights are being restricted in the name of a countervailing public interest. Respect of that 'essence' is paramount. Ignoring the 'essence' or the 'inalienable core' of these rights, ostensibly for the sake of protecting the health and life of citizens, would clearly be incompatible with the Charter.[7] Unsurprisingly, to liberally-minded States and individuals, the preferable method is to encourage citizens to behave in a way that serves both the collective good as well as their individual interest. This appears to be grounded in the presumption that if the threat is perceived to be serious enough, citizens will comply. This is a conundrum. There is ample evidence that people are ignoring the most serious warnings about COVID-19[8]; here is also evidence that the primacy of rules that suppress information (patient ethics and/or confidentiality, privacy or data protection) can have a negative effect on public health.[9] Nevertheless, foregoing democracy for an authoritarian regime is never the solution.

The use of contact-tracing apps has rightly raised many questions about the protection of users' privacy. It is axiomatic that the most privacy-preserving solution is not to deploy a contact-tracing app at all. Conversely, the most privacy-intrusive solution would be a compulsory app that provides a central authority with tracking and enforcement capabilities.[10] However, is either solution advisable? As it stands, the debate has been framed as follows: 'how do we build an app in the least privacy-intrusive way?" Unfortunately, the answer to this question may result in a version of the app that lacks adequate and effective functionality.

The balance of this post argues that coming to this problem from a 'privacy-preserving' perspective is the wrong approach and actually contradicts the letter of the law; in particular, the GDPR whose drafters envisaged public health emergencies would require alternative approaches to the processing of personal data and privacy. Accordingly, contact-tracing apps should be designed with the effectiveness of functionality in mind first, in compliance with data protection principles and with strong measures to protect and safeguard the rights and freedoms of data subjects imposed by law.

As it stands there is no discussion about mandating downloads. Yet effectiveness is said to engage the principles of necessity and proportionality under Article 8(2). However the cases on this point are limited to *covert* or otherwise *non-consensual surveillance*. Accordingly, public health experts should have been free to determine what is going to be the most adequate and effective way of building a contact tracing app that meets the aims and objectives of mitigating the effects of COVID-19. Only then should data protection experts and developers start to think about how to design the app in a privacy-preserving way.

Unsurprisingly, the focus thus far has been on whether the solution is 'privacy-preserving'. This

---

[5] Article 3, UN Declaration of Human Rights; Article 2, European Convention of Human Rights; Article 2, European Union Charter of Fundamental Rights and Freedoms

[6] Article 3, Charter of Fundamental Rights of the EU.

[7] For analysis see Maja Brkan, 'The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning' (2019) 20 German Law Journal 864.

[8] See for example, Coronavirus: Police fury as 'hundreds' of people have pizzas, beers and wine in park; Edinburgh police issue 32 fines and arrest five people as Covid-19 lockdown rules flouted | Edinburgh News; 'It's like a scene from Baywatch' - Beaches packed as lockdown is eased; Crowds gather at Portobello Beach on hottest day since lockdown began.

[9] For an interesting example, see the Scottish government's decision not to use contact-tracing to contact people attending/working at a Nike Conference in Edinburgh, Scotland under the auspices of patient confidentiality at https://www.bbc.com/news/uk-scotland-52722964?fbclid=IwAR3FK5ZO9C0QjTBkMl_LTqTYi3ghqD3s3pW1yOXLgAwS1k3vQErRv5NrlFs

[10] Qatar Has Made Its Coronavirus Contact Tracing App Mandatory at Qatar Makes Coronavirus Pandemic Tracking App Mandatory, (visited 22 May 2020).

approach is, in itself, a policy decision that can cost lives. As it stands, there are no measures provided for in either of the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) project or the Decentralised Privacy-Preserving Proximity Tracing (DP-3T) protocol that allow a central authority to enforce isolation or check whether users are actually heeding the advice to self-quarantine. Both initiatives are suspicious of big tech and government's surveillance capacities, while overwhelmingly trusting of citizens' compliance after notification of one's previous proximity to someone who has tested positive. This is also a policy decision not backed up with any actual evidence. There is nothing to suggest that users will comply on the basis of 'privacy-preserving' technology, while the tech's effectiveness is reliant on the compliance of its users.[11] Some argue that trust is needed for the uptake of contact-tracing apps (another assumption that has not been backed up with any evidence), while overlooking the fact that many will download simply for the app's utility and on the understanding that doing so will help facilitate a faster return to normality.

Yet in relation to public health responses, privacy does not save lives. The effectiveness of functionality backed up with enforcement and sanctions for non-compliance does. The first consideration, therefore, should have been, in the informed and expert opinions of the public health authorities and medical community, what functionality is needed to help prevent the spread of COVID-19? Understanding the needed functionality to achieve full effectiveness is also central to the legal consideration of whether an app passes the 'necessity' and 'proportionality' tests set out in human rights frameworks instruments and the GDPR. Second, many claim that necessity must be borne out of effectiveness; however, it is important to note that there are many unknowns about the way COVID-19 spreads. Conclusive information about what amounts to the most *effective* deployment of the app is not presently known. Therefore, a fully evidence-led policy for the development of contact-tracing apps is a luxury that is simply not available. Accordingly, the balance of this note will provide an examination of the implications of contact-tracing apps on human and fundamental rights while explicitly acknowledging that a) we are currently in a time of a recognized public health emergency requiring an urgent response.

- According to Article 8 of the EU Charter of Fundamental Rights ('EU Charter'):
    - "Everyone has the right to the protection of personal data concerning him or her."
    - "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."
    - "Compliance with these rules shall be subject to control by an independent authority."
- Furthermore, according to Article 52(1) of the EU Charter:
    - "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."
- Similarly, Article 8(2) of the European Convention on Human Rights ('ECHR'):
    - "There shall be no interference by a public authority with the exercise of [the right to respect for private and family life] except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of

[11] Less than 50% of people under 30 were "completely" complying with lockdown rules, according to the University College London (UCL) study" at Fewer young adults sticking to lockdown rules, UK study shows, (visited 22 May 2020).

others."

Taken together, the qualifications in the provisions above require that any interference with fundamental rights are:

(i) 'Provided for by law' (lawful)

(ii) The least invasive measures possible (proportionality)

(iii) necessary in a democratic society (necessity)

Furthermore, the General Data Protection Regulation (GDPR) lays down rules regarding lawfulness, proportionality and necessity. These provisions stipulate that the processing of personal data without the data subject's consent is prohibited unless 'necessary' for certain specified purposes:

- Article 6(1)(e): "Processing shall be lawful only if and to the extent that….: processing is **necessary** for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"; in other words, processing must be laid down by law and must be **necessary** for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller…..[that] law shall meet an objective of public interest and be **proportionate** to the legitimate aim pursued.
- Any contact-tracing app will be processing health data of data subjects. Under Article 9(1), the "processing of personal data….concerning health….shall be prohibited". However, this general prohibition on the processing of special categories of data is subject to certain exemptions: for example, the processing is **necessary** for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health….**on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject** (Article 9(2)(i) GDPR).
- Article 9(2)(j) GDPR also allows for health data to be processed when **necessary** for scientific research purposes or statistical purposes "in accordance with Article 89(1) based on Union or Member State law **which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject**."

Meanwhile the GDPR's Recitals provide further guidance about the changing role of the data protection framework during emergencies:

- Any processing of personal data necessary to protect lives is put on a lawful basis; more importantly, **surveillance** is *expressly permitted*:
    - **Recital 46:** The processing of personal data **should also be regarded to be lawful** where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. **Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, <u>including for monitoring epidemics and their spread or in situations of humanitarian emergencies</u>**, in particular in situations of natural and man-made disasters.
- Second, user consent is not needed during public health emergencies:
    - **Recital 54:** The processing of special categories of personal data may be necessary for reasons of public interest **in the areas of public health <u>without consent</u> of**

> **the data subject**. **Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons.** In this context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council (11), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest **should not result in personal data being processed for other purposes by third parties** such as employers or insurance and banking companies.

Taken together, the focus on '*privacy-preserving*' and *decentralization* goes *against* the intention of the drafters of the Regulation who clearly anticipated that, in the event of a public health emergency, data protection should not be standing in the way of effective functionality and frustrating the needs of authorities during an unprecedented public health crisis.

The basis for processing under Article 9(2)(i) indicates that the processing of 'special categories of personal data' like health data may take place without the consent of the data subject, provided such processing is necessary for the reasons stated therein and on the basis of a law which 'provides for suitable and specific measures to safeguard the rights and freedoms of the data subject'. Therefore, before rolling out any contact-tracing app, **member states have a legal obligation to introduce a law providing for suitable and specific measures to safeguard the rights and freedoms of the data subject.**

The wording of Recital 46 gives further indication that the prohibitive nature of the Articles 6 and 9 processing is an *ex ante* privacy-preserving measure, *in itself*. Furthermore, the explanation about how to apply the purpose limitation during crises found in Recital 54 should be seen as both an *ex ante* and *ex post* provision for protecting privacy. Thus, the GDPR should be seen as designed with public health crises in mind. As the text purposely shifts the emphasis onto the need for stronger safeguards, its drafters envisaged that the prohibitive structure of Article 9(1) would not be appropriate during a public health crisis. **Accordingly, privacy-preserving measures should be put on a lawful basis to ensure rights and freedoms and not on the front-end of the application where the functionality can be compromised in the name of 'privacy-preservation'.**

Any law to safeguard the rights and freedoms of the data subject should *inter alia* define who the controller/s is/are, specify the purpose of processing and lay down explicit limitations regarding further use, and enact appropriate and meaningful safeguards, including a specific reference to the voluntary nature of the application, provide specific rules for non-discriminatory protection[12], and an exit strategy (the measures must be temporary – not here to stay after the crisis). There should be strong measures and penalties for any data controllers/processors integrated into the law, with provisions guaranteeing deletion of any user data when the user no longer wishes to participate and/or the public health emergency is declared over.

There are emerging media reports that contact-tracing helped to 'flatten the curve' in South Korea[13];

---

[12] For example, any discrimination (e.g. denying the use of public transport) should be disallowed. "This would imply, in particular, that individuals who decide not to or cannot use such applications should not suffer from any disadvantage at all."- European Data Protection Board, Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak, Adopted on 21 April 2020.

[13] Test, trace, contain: how South Korea flattened its coronavirus curve at Test, trace, contain: how South Korea flattened its coronavirus curve, (visited 15 May 2020).

thus, providing some evidence about the effectiveness of contact-tracing.[14] Yet a key operational issue remains regarding the precise meaning of the '**necessity**' criterion in the provisions above. It should be noted that 'necessary' is **not** the same as 'indispensable'. In *Huber*[15], the CJEU assessed whether a centralized database was necessary in terms of *effectiveness*:

> "*...the centralisation of those data **could be necessary**, within the meaning of Article 7(e) of Directive 95/46, if it contributes to the more **effective** application of that legislation as regards the right of residence of Union citizens who wish to reside in a Member State of which they are not nationals.*" [**Emphasis Added**]

Although this judgment interprets Article 7(e) of Directive 95/46 (its equivalent is now found in Article 6(1)(e) GDPR), the terminology of 'processing is necessary....' is reproduced verbatim; accordingly, the same interpretation ought to be applied if a new case arises that requires a similar assessment. Moreover, this interpretation is in line with the jurisprudence of the European Court of Human Rights ('ECtHR'). The ECtHR has stated that 'the adjective "necessary" is **not synonymous** with "indispensable".[16] In Judge Mosler's separate opinion he stated:

> *"Such a definition would be too narrow and would not correspond to the usage of this word in domestic law. On the other hand, it is beyond question that the measure must be appropriate for achieving the aim. However, a measure cannot be regarded as inappropriate, and hence not "necessary", just because it proves ineffectual by not achieving its aim."*[17]

In the words of the ECtHR in *Silver and Others v the United Kingdom*[18]:

> "*On a number of occasions, the Court has stated its understanding of the phrase 'necessary in a democratic society', the nature of its functions in the examination of issues turning on that phrase and the manner in which it will perform those functions. It suffices here to summarise certain principles: (a) the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable"*

This contradicts the common misperception that 'necessary' = 'indispensable' (or 'must have'). This argument, often deployed by privacy advocates, is wrong *even* in the context of ***covert, non-consensual surveillance*** activities by state security agencies, which is the context of that jurisprudence of the ECtHR. The judgments of the ECtHR also clarify the 'margin of appreciation' available to national authorities:

> '*the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved*'.[19]

In the context of covert, non-consensual surveillance by state security agencies, the ECtHR has held that:

> *'the margin of appreciation available to the respondent State in assessing the pressing social need in the present case, and in particular in choosing the means for achieving the legitimate aim of protecting national security, was a wide one'*[20].

---

[14] How South Korea Reined In The Outbreak Without Shutting Everything Down, at https://www.npr.org/sections/goatsandsoda/2020/03/26/821688981/how-south-korea-reigned-in-the-outbreak-without-shutting-everything-down, (Visited 15 May 2020).
[15] Case C-524/06
[16] *Handyside v UK* (1976) 1 EHRR 737 at 48
[17] Ibid. Separate opinion of Judge Mosler
[18] (1983) 5 EHRR 347 [97]:
[19] Leander (1987) 9 EHRR 433 [59].
[20] *Ibid.* For an example of this, see 'Dutch government working on emergency law to use telecom network data' at Dutch government working on emergency law to use telecom network data, (visited 23 May 2020).

In the extraordinary situation of a pandemic, the margin of appreciation available to State parties in assessing what is necessary for fulfilling that aim is also wide. It should also be noted that, in the present analysis, we are not faced with an instance of covert or otherwise non-consensual processing of personal data (as were the circumstances in the case-law discussed above), but rather with the consensual uptake of an app that users voluntarily sign up to for the purposes of assisting the State during a public health crisis. While there is as yet no case-law on this point, the voluntary nature of the processing throws into doubt the very existence of an interference with the rights laid down in Article 8(1) ECHR.[21]

Together with Article 9(2)(h) and (j) in certain circumstances and depending on the design and utility of the app, Articles 6(1)(e) and 9(2)(i) GDPR are really the only grounds of processing that matter. As long as it remains non-compulsory, choosing to download a contact-tracing app is no different than choosing to download Google Maps. With European countries set to deploy some form of contact-tracing app, it will simply come down to whether users *trust* the people responsible for the app's deployment and feel an obligation to do so through some sense of civic responsibility. Of course, privacy and data protection are an important part of earning this trust. However, these trust-building elements can come about on the front end at the expense of functionality, or on the back end through strong safeguards as required under Article 9(2)(i).

Acceptance of contact-tracing depends on a combination of technological characteristics, as well as legal variables; for example, the more transparent the surveillance technology is at the border, the more acceptable it is to travellers.[22] It is also posited that trust is intrinsically linked to privacy.[23] But there is more than one means to achieve this end and there is more than one way to ensure privacy: put effective functionality first (trusting that the app has worthwhile utility to justify the interference with privacy), second, ensure the user interface is friendly and understandable second (by ensuring the app is friendly and easy to navigate, users trust what is going on inside the environment); third, design apps for compliance with the GDPR's principles, while ensuring strong privacy and data protection safeguards are put on a *lawful* basis.

Back in 2013, Professor Andrew Murray of the London School of Economics made a keynote speech to the conference attendees of BILETA (British Irish Law and Education Technology Association) in which he encouraged 'cyberlawyers to re-engage with traditional jurisprudential models and thus to make ourselves relevant to lawmakers and lawyers'.[24] Mindful of his call to arms, it is worth noting that there is a way to achieve privacy beyond design - using law. We should take stock of this in our obligation to reflect how we responded to the threat of COVID-19.

END OF THIS PART OF THE ARTICLE

[21] cf. Lee A. Bygrave, *Data Privacy Law: An International Perspective*, (OUP 2014) at 91
[22] Didier Bigo, 'Globalized (in)security: The field and the ban-opticon' in Didier Bigo & Anastassia Tsoukala (eds), *Terror, Insecurity and Liberty. Illiberal practices of liberal regimes after 9/11* (Routledge 2008) 10 - 48.
[23] See for e.g. "The EDPB firmly believes that, when processing of personal data is necessary for managing the COVID-19 pandemic, data protection is indispensable to build trust, create the conditions for social acceptability of any solution, and thereby guarantee the effectiveness of these measures." EDPB Guidelines 04/2020
[24] http://theitlawyer.blogspot.com/2013/04/my-keynote-address-to-bileta.html