INSIGHTS

POLICY FORUM

TECHNOLOGY GOVERNANCE: COVID-19

What's next for COVID-19 apps? Governance and oversight

Adaptive governance can help earn social license

By **Alessandro Blasimme** *and* **Effy Vayena**

Many governments have seen digital health technologies as a promising tool to address coronavirus disease 2019 (COVID-19), particularly digital contact tracing (DCT) apps such as Bluetooth-based exposure notification apps that trace proximity to other devices (*1*) and GPS-based apps that collect geolocation data. But deploying these systems is fraught with challenges, and most national DCT apps have not yet had the expected rate of uptake. This can be attributed to a number of uncertainties regarding general awareness of DCT apps,

privacy risks, and the actual effectiveness of DCT, as well as public attitudes toward a potentially pervasive form of digital surveillance. DCT thus appears to face a typical social control dilemma. On one hand, pending widespread uptake, assessing DCT effectiveness is extremely difficult; on the other hand, until DCT effectiveness is proven, its widespread use at a population scale is hard to justify. Recognizing that technological uptake is an open-ended process reliant upon social learning and the piecemeal creation of public trust, we suggest that policy-makers set up mechanisms to test effectiveness, oversee the use of DCT apps, monitor public attitudes, and

adapt technological design to socially perceived risks and expectations.

To date, both scholarly and policy debates on DCT have largely overlooked the above dilemma, focusing instead on privacy-related issues as the pivotal element of DCT governance (*2*). However, although preserving privacy is of the utmost importance, technical safeguards such as encryption, decentralized data architectures, and temporal limits to data storage have not proved sufficient for DCT apps to quickly diffuse at a population scale.

Social license and trust depend on the capacity of either corporations or governments to meet societal expectations in relation to a specific activity (*3*). Therefore, for DCT to earn social license, such expectations, as well as the factors that cause slow uptake on the part of the public, need to be probed. To increase public trust, the World Health Organization has stressed the importance of

Health Ethics and Policy Lab, Department of Health Sciences and Technology, ETH Zurich, Zurich, Switzerland. E-mail: effy.vayena@hest.ethz.ch; alessandro.blasimme@hest.ethz.ch

appropriate oversight for the governance of DCT apps (*4*). Switzerland, for example, has involved the Federal Data Protection and Information Commissioner and the Federal Ethics Committee in the development of the Swiss national DCT app. The French government has sought advice from eight high-profile national expert bodies. Such moves can contribute to the legitimation of a country's approach to DCT. Likewise, oversight mechanisms of a DCT app can play a role in sustaining widespread and continued use by the public.

PUBLIC RELUCTANCE

Studies conducted in April and May 2020 showed that in countries like the United States, Switzerland, and Italy, between 55 and 70% of adults in all age groups were willing to download a contact tracing app (*5*). Yet these figures do not match the current DCT apps uptake. Even in countries with robust privacy safeguards in place, downloads of DCT apps have been below expectations. At the time of writing, the Australian DCT app has been downloaded by 6.5 million (26% of the population), the Italian one by 8 million (13.4%), and the newly released French one by 1.5 million (2.3%). Ireland has about 1.3 million active app users (24%), Switzerland 1.8 million (21.5%), and Germany 16 million (19.3%). As people keep downloading the app, at some point, the desirable number of users may be reached. Decades of research in science and technology studies confirm that such a bell-shaped innovation diffusion pattern is not particularly surprising, as technological uptake does not just rapidly happen by virtue of a technology's presumed usefulness (technological determinism), but owes instead to complex cycles of cultural and political adaptation (social construction of technology) (*6*).

Members of the public cite unauthorized uses of their data beyond COVID-19 containment and access to personal data by IT companies and state authorities as matters of concern (*7*). Moreover, older people and people of lower socioeconomic conditions are considerably less likely to download DCT apps (*8*). Although the public's reservations are understandable, efforts should be made to respond to those concerns and increase the rate of early adoption of DCT systems. Use of opt-out mechanisms rather than opt-in, and large cohort studies in which participants are incentivized to try out the app, could boost initial uptake across demographics. This would help address the dilemma discussed above, leading to a parallel increase in the capacity to assess effectiveness and, at the same time, to exert control over such systems. Failure to do so could lead to premature dismissal of a potentially useful new technology. The Norwegian data protection authority, for instance, stated that the known risks of DCT surveillance outweigh its still unproven public health benefits—a position that caused the Norwegian government to put the system on hold (*9*).

ADAPTIVE GOVERNANCE

When technologies come with known risks but uncertainties about benefits persist, adaptive governance is a valuable policy option. It has a long and respected pedigree—both in academic scholarship and in policy-making—including in areas that resemble severe public health crises, such as natural hazards and disaster risk reduction. In the case of DCT, we know that privacy-related risks are present, alongside risks linked to public surveillance and to technical failure in the presence of a global public health threat. At the same time, DCT effectiveness in containing damage from COVID-19 is still to be assessed.

According to adaptive models, governance should enable social learning and distribute oversight tasks across different actors (*10*). Collaboration between different stakeholders such as developers, health ministries, data protection authorities, experts, and the involvement of lay publics is a key element for an efficient adaptive governance approach (*11*). In the face of the above uncertainties, adaptive governance urges national DCT initiatives to collect and rapidly incorporate new knowledge into their governance.

To effectively implement adaptive governance of DCT, oversight activities should focus on a number of specific adaptive features (*11*, *12*).

Public engagement

Owing to the exceptional circumstances of the COVID-19 crisis, national DCT plans have been rolled out without engaging the public in any phase of the process (*13*). In democratic countries, this is likely to undermine trust in technological solutions, especially if they embody a pervasive surveillance logic that may well appear at odds with democratic ideals. DCT initiatives should thus ensure that they offer regular opportunities of democratic input into the governance of DCT. This can be guaranteed by including lay publics such as civil society representatives, advocacy groups, and non-governmental organizations in oversight bodies. Moreover, surveys, deliberative forums, and notice-and-comment periods should be regularly offered to increase public input into the governance of national DCT apps. Public engagement should not be seen as a legitimation tool alone, but as a fundamental component of the adaptation process, a precondition for social learning around both anticipated and unanticipated risks. Moreover, public engagement has the potential to mitigate the threat posed by incumbent concentrations of power by state authorities or private companies involved in national DCT strategies.

Technical aspects

The effectiveness of DCT systems in breaking transmission chains should be assessed against previously established public health objectives, such as app penetration, accuracy, and effectiveness in reducing the health and social burden of the infection. Failure to meet these objectives should lead to reconsidering specific technical aspects of existing DCT strategies.

Regular monitoring of technical parameters about the use and reliability of DCT apps would inform specific strategies to be adopted to increase the rate of downloads and actual use of the apps, and to improve their functioning. Most DCT apps are built with a proactive commitment to privacy-preserving technological features (privacy by design) and only use strictly necessary data (privacy by default). However, no privacy-preserving system is perfect. Oversight bodies should thus regularly test the robustness of adopted privacy-preserving measures and define plans to continuously minimize harms.

Legal aspects

DCT oversight should be able to clarify or, as the case may be, suggest legal definitions for the kind of data collected by DCT apps and the specific roles of all the actors—private or public—involved in development and implementation. In particular, specific types of data like rotating Bluetooth IDs or associated metadata may not have a clear legal status in a given jurisdiction. Ad hoc legislation may also be needed to set specific rules and safeguards around voluntariness and misuses of DCT tools. In Switzerland, for example, such legal provisions were introduced in an amendment to the Epidemics Act before the release of the national DCT app.

Sanctions linked to unlawful handling of personal data are present in most jurisdictions. Increasing public awareness about such legal consequences of data misuse can support trust in DCT systems.

DCT apps operate within national territories. However, cross-border use would facilitate contact tracing while reinstating global mobility. To achieve this objective, technical interoperability and specific legal safeguards about cross-border data

exchange must be adopted. The European Commission recently published the "European Interoperability Certificate Governance" specifying technical standards that will enable safe data exchange between national apps (14).

Moreover, DCT is not limited to state-sponsored national apps. Private-sector employers and small businesses are already developing their own internal contact tracing systems, and they may make them mandatory for workers and customers. This is happening in the absence of specific legal provisions. DCT oversight bodies should therefore suggest policy guidance to ensure that such private-sector DCT is aligned with constitutional rights and freedoms and will not be used to unduly monitor employees and private citizens. Failure to deploy appropriate regulatory frameworks for private-sector DCT may undermine trust in DCT broadly.

Ethical aspects

If DCT gains traction, ethically complex trade-offs between privacy and effectiveness, or between users' expectations and utility, may need to be addressed. For instance, as new clusters of infection emerge, DCT data may be used to study epidemic dynamics in real time. But this may require lowering privacy safeguards to grant public health authorities access to DCT data. Oversight bodies should thus have monitoring and auditing capacity to ensure that exhaustive information about the scope of data use and data protection safeguards is properly communicated to users through a meaningful electronic informed consent process. Existing guidance on the use of electronic informed consent (15) should be adapted to DCT, ensuring that ethical requirements are fulfilled and appropriate ethics review is conducted. Oversight bodies will also have to regularly probe public attitudes and advise policy-makers as to ethically justified, socially accepted, and proportional solutions to such issues.

Notably, DCT runs the risk of exacerbating health inequalities by missing out on people who either do not have a smartphone, have contracts for limited data use, or are not proficient users. Frequently, elders are unfamiliar with advanced smartphone features and may thus be excluded from the potential benefits of DCT—despite representing the most vulnerable social group in terms of COVID-19–related mortality. Furthermore, social groups that are more open to using DCT apps may be taking on a disproportionate burden in making themselves traceable. DCT oversight bodies should be able to monitor these risks and propose, where appropriate, an equitable distribution of the benefits and burdens of DCT. To this aim, it is advisable to include social scientists in oversight bodies, with a mandate to monitor how different social groups respond to and are affected by DCT activities.

REFLEXIVE ADAPTATION

In all of the above domains, oversight bodies should foster reflexive adaptation (11, 12) of DCT strategies based on real-world data on actual use of DCT apps. Reflexive adaptation consists in regularly questioning assumptions about design, risks, and users' attitudes to adapt technological features.

One way to proceed is to pay close attention to opportunity costs of new DCT technologies. This implies assessing regularly whether DCT complements or foregoes other containment strategies such as manual tracing methods of established effectiveness—for example, on grounds of representing a cheaper alternative.

Moreover, reflexivity amounts to the capacity to leverage social learning to detect emerging patterns of discrimination and unfair treatment—faced, for instance, by nonusers and people who do not possess the latest smartphone models, or can only afford low–data-use contracts. A further element requiring reflexive capacity is the possible normalization of digital surveillance within and beyond the realm of public health. For instance, DCT apps could be developed to incorporate functions, e.g., QR codes for entry to facilities, that also enable contact tracing—as lately seen in China and the United Kingdom. Unrolling such pervasive forms of control might generate habituation to their use in other domains such as work, schools, public transportation, and so on. Reflexive vigilance of these potential long-term effects is of the utmost importance to prevent the erosion of civil liberties and human rights.

A further hallmark of reflexive adaptation is the capacity to question basic assumptions of DCT models regarding, for instance, users' risk-related behaviors. Although it is generally assumed that DCT alerts are empowering for individuals, different people have different ways of making sense of risk. Absent appropriate user behaviors, the actual effectiveness of DCT will likely be limited. It is therefore important to collect evidence that helps clarify how users act upon being notified by a DCT app. This evidence can be used in efforts aimed at sensitizing users to follow best practices and recommendations about testing and self-isolation.

ROBUST OVERSIGHT

The rapid deployment of DCT apps represents one of the largest experiments in public health surveillance ever attempted—and certainly the first one relying so strongly on digital platforms. We have argued that DCT governance should be focused on evidence collection and planned adaptation to address numerous uncertainties. In the context of a global crisis requiring rapid responses, this approach has two further advantages: It allows governance structures to coevolve with technological solutions while they are already in use, and it can reduce the high cost of intervening in an already widespread technology.

Whatever form, mandate, and composition individual countries will establish, the creation of oversight structures around DCT is of paramount importance and cannot be delayed. Robust oversight will nurture public trust and will contribute to stronger ethical safeguards and to the assessment of DCT's contribution to a safer coexistence with the virus until effective vaccines become available.

COVID-19 found the world unprepared, but now it is time for governments to carefully predispose all the necessary measures to boost resilience and minimize future harms. This model will arguably be useful for other technologies and in case of future large-scale crises—in public health and possibly beyond. ■

REFERENCES AND NOTES

1. I. G. Cohen, L. O. Gostin, D. J. Weitzner, *JAMA* **323**, 2371 (2020).
2. U. Gasser, M. Ienca, J. Scheibner, J. Sleigh, E. Vayena, *Lancet Digital Health* **2**, e425 (2020).
3. J. Morrison, *The Social License* (Palgrave MacMillan, 2014).
4. "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing" (2020); www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1.
5. E. Hargittai, E. Redmiles, *Sci. Am.* (2020); https://blogs.scientificamerican.com/observations/will-americans-be-willing-to-install-covid-19-tracking-apps/.
6. W. E. Bijker, T. P. Hughes, T. J. Pinch, *The Social Construction of Technological Systems* (MIT Press, 1987).
7. Ipsos MORI, "Survey on COVID-19 track and trace smartphone app for The Health Foundation" (2020); www.ipsos.com/ipsos-mori/en-uk/survey-covid-19-track-and-trace-smartphone-app-health-foundation.
8. Ipsos MORI, "Demographic divide in likelihood to download and report symptoms on the Government's contact tracing app" (2020); www.ipsos.com/ipsos-mori/en-uk/demographic-divide-likelihood-download-and-report-symptoms-governments-coronavirus-contact-tracing-app.
9. G. Ursin, I. Skjesol, J. Tritter, *Health Policy Technol.* (2020).10.1016/j.hlpt.2020.08.004
10. C. Folke, T. Hahn, P. Olsson, J. Norberg, *Annu. Rev. Environ. Resour.* **30**, 441 (2005).
11. E. Vayena, A. Blasimme, *J. Law Med. Ethics* **46**, 119 (2018).
12. A. Blasimme, E. Vayena, in *Oxford Handbook of Ethics of AI*, F. Pasquale, M. Dubber, S. Das, Eds. (Oxford Univ. Press, 2020), pp. 703–718.
13. M. M. Mello, C. J. Wang, *Science* **368**, 951 (2020).
14. European Commission, European Interoperability Certificate Governance: A security architecture for contact tracing and warning apps; https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_certificate_governance_en.pdf.
15. *Fed. Regist.* **81**, 90855 (2016).

10.1126/science.abd9006

Science

What's next for COVID-19 apps? Governance and oversight

Alessandro BlasimmeEffy Vayena

View the article online
Permissions