Digital tools against COVID-19: taxonomy, ethical challenges, and navigation aid

Urs Gasser, Marcello Ienca, James Scheibner, Joanna Sleigh, Effy Vayena

Data collection and processing via digital public health technologies are being promoted worldwide by governments and private companies as strategic remedies for mitigating the COVID-19 pandemic and loosening lockdown measures. However, the ethical and legal boundaries of deploying digital tools for disease surveillance and control purposes are unclear, and a rapidly evolving debate has emerged globally around the promises and risks of mobilising digital tools for public health. To help scientists and policy makers to navigate technological and ethical uncertainty, we present a typology of the primary digital public health applications that are in use. These include proximity and contact tracing, symptom monitoring, quarantine control, and flow modelling. For each, we discuss context-specific risks, cross-sectional issues, and ethical concerns. Finally, recognising the need for practical guidance, we propose a navigation aid for policy makers and other decision makers for the ethical development and use of digital public health tools.

Lancet Digital Health 2020; 2: e425–34

Published Online
June 29, 2020
https://doi.org/10.1016/S2589-7500(20)30137-0

Berkman Klein Center for Internet & Society, Harvard Law School, Harvard University, Cambridge, MA, USA (U Gasser PhD); **and Health Ethics and Policy Laboratory, Department of Health Sciences and Technology, Swiss Federal Institute of Technology in Zurich, Zurich, Switzerland** (M Ienca PhD, J Scheibner PhD, J Sleigh MA, Prof E Vayena PhD)

Correspondence to:
Prof Effy Vayena, Health Ethics and Policy Laboratory, Department of Health Sciences and Technology, Swiss Federal Institute of Technology in Zurich, Zurich 8092, Switzerland
effy.vayena@hest.ethz.ch

Introduction

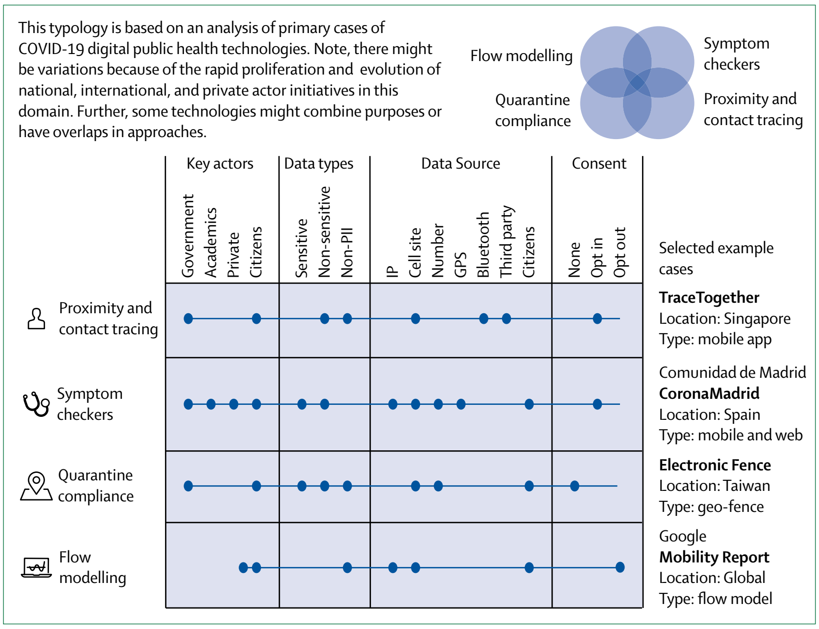
The collection and use of data is presented as a key strategic remedy by governments and private actors in response to the COVID-19 pandemic. Across countries and institutions, public health experts and researchers from diverse fields such as epidemiology, virology, evolutionary biology, and social science have pointed out the broad range of insights that can be gained by collecting, analysing, and sharing data from diverse digital sources. These sources include data from telephone towers, mobile phone apps, Bluetooth connections, surveillance video, social media feeds, smart thermometers, credit card records, wearables, and several other devices. In parallel, Apple and Google, two of the world's largest information technology companies, have unprecedentedly banded together to create application programming interfaces that enable an interoperability between Android and iOS devices using apps from public health authorities, to offer a broader Bluetooth-based exposure notification platform by building this functionality into the underlying platforms.[1]

Although the promise of big data analysis has been widely acknowledged, and governments and researchers around the globe are rushing to unlock its potential, notable technical limitations have also surfaced. These limitations include the accuracy, granularity, and quality of data that vary greatly across the different data sources; the adequacy of computation safeguards; and the interoperability issues and security risks. Simultaneously, notable ethical and legal risks and concerns have been identified that accompany digital disease surveillance and prediction.[2] Civil rights organisations, data protection authorities, and emerging scholars have highlighted the risk of increased digital surveillance after the pandemic.[3] These groups have emphasised the need to meet baseline conditions such as lawfulness, necessity, and proportionality in data processing, and the need for social justice and fairness to take precedence despite the urgency of this crisis.

As many public and private sector initiatives aiming to use digital technologies in the fight against COVID-19 emerge, the ensuing debate so far seems to be framed generically in a binary choice between using digital technologies to save lives and respecting individual privacy and civil liberties. However, interdisciplinary research has shown the value of context in managing the societal, legal, and ethical risks of data processing for pandemics that stretch beyond the issue of privacy.[4–7] In this Health Policy paper, we seek to contribute to the rapidly evolving debate about the promises and risks of digital public health technologies in response to COVID-19. Rather than a focus on so-called solutionist or instrumentalist approaches (where the focus is on the benefit that the technology itself brings to public health management) to digital public health technologies, we instead focus on public health outcomes, as well as the ethical principles guiding these outcomes.[8] We offer a typology of the main applications that are in use, and we discuss their respective features, including both application-specific and context-specific risks, cross-sectional issues, and ethical concerns. Finally, we propose a navigation aid for policy makers, recommending steps that should be taken to mitigate risks by engaging in a robust risk–benefit analysis. This aid is derived from the translation of ethical principles from public health and data ethics, and builds upon process-based risk assessment and governance frameworks. Further, this aid can be calibrated to each typological domain to guide different technological platforms and at various phases of the deployment of digital public health technology.

Typology of digital public health tools

Using an established analytical framework for the creation of categorical variables,[9] we reviewed the rapidly evolving spectrum of digital public health technologies against COVID-19 and created a multidimensional descriptive typology (figure 1). This typology is based on four main categorical variables: key actors, data types, data source, and model of consent. The concept measured by the typology (called the overarching concept in typological research) is the public health



This typology is based on an analysis of primary cases of COVID-19 digital public health technologies. Note, there might be variations because of the rapid proliferation and evolution of national, international, and private actor initiatives in this domain. Further, some technologies might combine purposes or have overlaps in approaches.

	Key actors				Data types			Data Source							Consent			
	Government	Academics	Private	Citizens	Sensitive	Non-sensitive	Non-PII	IP	Cell site	Number	GPS	Bluetooth	Third party	Citizens	None	Opt in	Opt out	Selected example cases
Proximity and contact tracing	●			●		●	●		●			●	●			●		**TraceTogether** Location: Singapore Type: mobile app
Symptom checkers	●	●	●	●	●	●		●	●	●	●			●		●		Comunidad de Madrid **CoronaMadrid** Location: Spain Type: mobile and web
Quarantine compliance	●			●	●	●	●		●	●				●	●			**Electronic Fence** Location: Taiwan Type: geo-fence
Flow modelling			●	●			●	●	●					●			●	Google **Mobility Report** Location: Global Type: flow model

***Figure 1:* Typology of digital public health technologies against COVID-19**
IP=Internet Protocol. GPS=Global Positioning System. PII=Personally Identifying Information.

function of a technology; not its physical realisation at the hardware or software level. As a result, this multidimensional model can be put in use to categorise not only tools that have already been deployed but also future and emerging technologies. Our typology identifies four main functional categories of digital public health technologies for pandemic management: proximity and contact tracing, symptom monitoring, quarantine control, and flow modelling.

Proximity tracing tools measure the spatial proximity between users to track their interaction. Proximity tracing, sometimes also in conjunction with patient reports or other non-digital sources, can identify when users are exposed to an individual that is positive for severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). For example, the Singaporean application TraceTogether uses Bluetooth connections to log other telephones nearby and alerts those who have been close to an individual who is SARS-CoV-2 positive. When users have shared proximal space with someone who is SARS-CoV-2 positive, they are encouraged to self-isolate.[10]

Symptom checkers are tools of syndromic surveillance that collect, analyse, interpret, and disseminate health-related data.[11] Using these tools, users report their symptoms, obtain a diagnosis, and possibly get a triage decision. Accordingly, symptom checkers promise a cost-effective way of enabling rapidly scalable epidemiological data collection and analysis, which is crucial for a data-driven response to this public health challenge.[12] Further, the value of digital symptom checkers resides in their assistance in triaging large international and disperse populations of patients that seek health care. An example of a symptom checker is the CoronaMadrid symptom checking application. Using this technology, the Spanish Government collaborated with citizens, health professionals, and the private sector to monitor the disease, respond quickly, allocate resources, and generally minimise or control outbreaks. Another mobile application called the COVID-19 Symptom Tracker garnered more than 2·8 million users in the UK and the USA, collecting data on risk factors, symptoms, clinical outcomes, and geographical hot spots to inform a data-driven response to this public health challenge.[12]

Quarantine compliance tools involve the real-time monitoring of whether individuals who are symptomatic or non-symptomatic are complying with quarantine restrictions. Public health legislation includes requirements for infected or potentially infected individuals to be isolated from others, so they do not spread the disease further. These technologies can provide a mechanism of ensuring that infected individuals are isolated from other individuals. Examples include Taiwan's Electronic Fence application that tracks quarantined overseas arrivals using mobile phone data.[13]

Flow modelling tools, otherwise known as mobility reports, quantify and track people's movements in specified geographical regions. Typically, these tools rely on aggregated, anonymised sets of data from the geographical location of users. Flow modelling can provide insight into the effectiveness of response policies (eg, physical distancing or forced quarantine) aimed at combating COVID-19.[14]

This typology allows us to structure these technologies in a four-dimensional model. First, we include the key actors involved in the design and implementation of these technologies (government agencies, academia, private companies, and citizens). Secondly, we assess the different data types being collected, using the classification offered by the General Data Protection Regulation (EU) 2016/679 (non-identifying personal data, and sensitive personal data). Thirdly, our typology includes the different origins of these data, including Internet Protocol addresses, call site data, Global Positioning System data, Bluetooth, and third-party data. Finally, this typology considers the different types of consent required to collect data, including opt-in consent, opt-out consent, and mandatory use. This four-dimensional model allows us to compare the ethical implications of different types of technological approaches to pandemic management, as shown in figure 1. Note, there might be variations of these technologies and overlaps in approaches because of the rapid proliferation and evolution of national, international, and private actor initiatives in this domain.

Further, it should be highlighted that the digital health tools mentioned already, because of their reliance on different data types and sources, are differently affected by potential barriers to wide-scale adoption. Flow modelling tools such as Google's

COVID-19 Community Mobility Reports are more likely to be adopted widely because they are created with aggregated data from users who have turned on the location history setting but are not required to download any additional software. Proximity tracing tools, in contrast, typically require the user to download an application from an application store and to create a user account. Early assessments in countries like India, Norway, and Singapore have shown that low uptake hampers efforts to use this technology.[15]

Mapping ethical and legal challenges

These four types of digital public health technologies raise ethical–legal considerations that are both cross-sectional and domain-specific. These considerations are grounded in the basic principles and moral considerations of public health ethics and data ethics, in particular the principles of autonomy, justice, non-maleficence, privacy, and solidarity (figure 2).[16–19] By translating these principles and values into the context of digital public health technologies, we identified the following ethical and legal challenges for researchers and policy makers.

Ensuring public benefit

Underpinning all scientific, ethical, and legal challenges of pandemic management is the question of public benefit. Similar to any other health-care intervention such as medicines or lockdown measures, the rollout of digital public health tools to combat the pandemic requires a reasonable expectation of public benefit (ethical principle of beneficence) and clear prospective evidence that such benefit will outweigh the risks (non-maleficence). Possible benefits associated with these technologies include forecasting new outbreaks,[20] promptly alerting and isolating exposed individuals and thereby preventing or reducing new infections, improving quarantine measures, improving the efficiency of social care and vaccine development, and improving how information is communicated to citizens.[21] The realisation of these benefits might depend on technology-specific factors. For example, simulation data suggest that the beneficial impact of contact tracing apps largely depends on the user uptake rates being more than 50% of the population,[22] which have not yet been achieved by any existing technology. Symptom checkers, in contrast, appear more rapidly scalable but might be affected by data quality issues since they are typically based on self-reported data.[12] In addition, as emphasised earlier, the efficiency might depend on many non-technical factors, including the availability of testing, socioeconomic affordances (eg, social safety nets for people affected by the lockdowns) and public trust.[23,24] In general terms, in order to ensure the public benefit of a digital public health technology, developers and deployers must make choices towards a clearly favourable risk–benefit ratio throughout the different phases of the decision making process as outlined in figure 2.

This sunburst diagram presents how the six ethical principles raise ethical and legal issues when considered in relation to digital public health technologies against COVID-19. As shown by the intersecting circles at the centre, these principles apply equally to symptom checkers, proximity and contact tracing, quarantine compliance, and flow modelling.

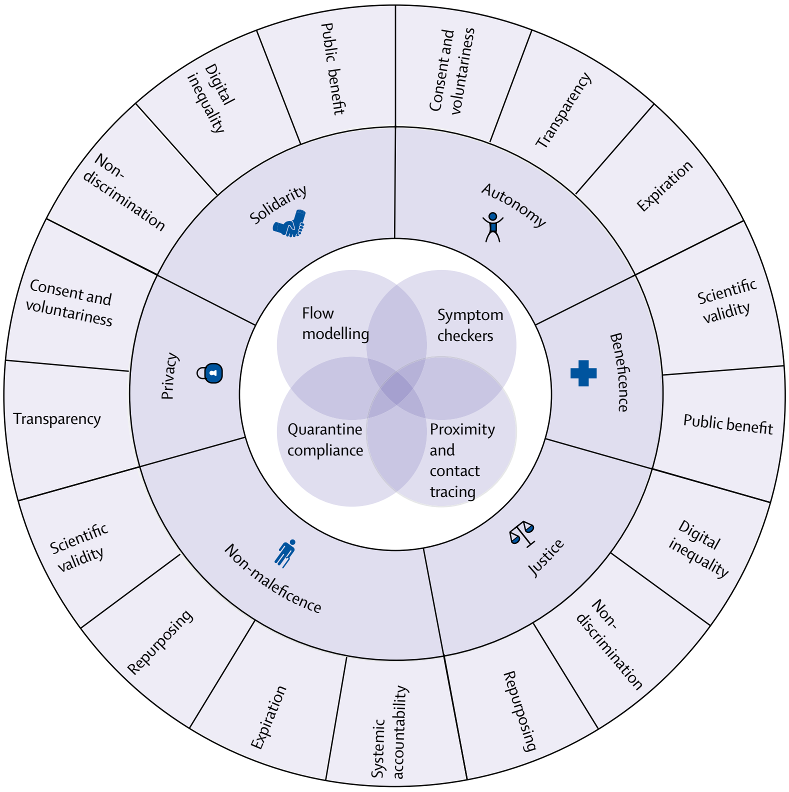


Figure 2: **Sunburst diagram mapping the ethical and legal issues raised by applying ethical principles to COVID-19 digital public health technologies**

Ensuring scientific validity and accuracy

Despite widespread enthusiasm about using novel digital public health technologies to combat epidemics, there is little scientific evidence of their efficacy to date.[25] For example, smart phone applications for COVID-19 proximity and contact tracing are being rolled out in many countries after few, if any, pilot studies or risk assessments being published.[25] In the absence of official validation tests and protocols there can be no indicator of accuracy and effectiveness. However, the urgency of the ongoing pandemic is no justification for lowering scientific standards. By contrast, it heightens the responsibility of public health actors to uphold rigorous and evidence-based practices.[26] Furthermore, the use of digital tools involves inevitable compromise. Even when digital public health technologies can demonstrably improve the rapidity of pandemic response[27] they might nonetheless be affected by issues of data quality and integrity that, in turn, can have an outsized effect on large-scale predictive models.[28] Uncertainty about scientific efficacy can make assessing the proportionality and risk of proposed measures more challenging.[29] Subsequently, measures based on such models might be disproportionate, negatively affecting individuals and populations without generating notable benefits. Although several global actors are independently pursuing digital public health strategies, typically at the country level, it is crucial to ensure the interoperability of such digital systems and enable efficient, harmonised, and secure cross-national data sharing. This pandemic is a global challenge, hence cannot be tackled only locally and requires new cooperative approaches.

Protecting privacy

All digital public health tools impinge upon individual privacy by requiring some degree of access to information about the health status, behaviour, or location of individuals.[30] However, privacy risks vary across our typology depending on the purpose and data types used by a digital tool. Digital tools for measuring relative spatial proximity among phone users are, all other things being equal, less privacy-invasive than personal contact tracing or quarantine enforcement apps. Likewise, tools using aggregate mobile phone tower data are, on average, less privacy-invasive compared with tools based on Global Positioning System data and sensor tracking for individual users.[31] The use of more granular and specific types of data can increase the risk of downstream reidentification of individuals or groups. Further, with the vast amount of data being gathered, public health agencies and application developers must prevent downstream reidentification through data linkage.[32] It is also vital to understand that privacy risks can change and accumulate over time, which highlights the need for strong legislative protection. In the EU, several regulatory instruments offer varying amounts of safeguards for the right to privacy and data protection. These include the General Data Protection Regulation, the e-Privacy Directive and the Charter of Fundamental Rights. Likewise, at the Council of Europe level, the European Charter of Human Rights guarantees the right to a so-called private life. However, these regulations set forth the circumstances where these rights can be abridged, including during a public health crisis, and several EU institutions have provided relevant guidance recently.[33] Further, any digital public health technologies abridging these rights must be proportionate to the aims sought. In other words, this abridgment must lead to a faster restoration of other rights and freedoms that were suspended because of lockdown policies (eg, freedom of movement and freedom of assembly).[34]

Preserving autonomy

Digital public health technologies have the potential to undermine not only privacy but also personal autonomy. The most obvious form of violation of personal autonomy is the mandatory use of digital public health technologies. For example, India's home ministry has required that all local workers, public or private, use a government-backed COVID-19 tracking application called Aarogya Setu.[35] However, even when governments do not make the use of such technologies mandatory, it is conceivable that organisations or employers might require their use for particular activities or access to services. In such cases, people will be left with no real option and their autonomy will be undermined. Less explicit threats to autonomy are raised by smart phone applications that include permissions to collect data beyond the stated purpose of the application. These data handling practices might strip people of their ability to consent to being tracked or having their information shared, depending on their purpose, mode of data collection, and data source. For example, in order to work properly, proximity tracking apps based on Bluetooth need to require or encourage users to keep their Bluetooth turned on at all times, creating additional risks. These approaches to data collection must respect autonomy, such as by ensuring strategies are in place to update the user regularly. Finally, mandating quarantine apps or technologies for infectious individuals or their contacts raises the most serious questions of justifiable coercion. On the one hand, the effectiveness of quarantine might be undermined if it remains voluntary rather than mandatory. On the other hand, some government activity (such as the Polish government creating shadow profiles for returning citizens as part of a quarantine app) might constitute an overreach on autonomy.[36]

Avoiding discrimination

Along with the risk of reidentification and infringement of personal autonomy, digital public health technologies also carry an inherent risk of discrimination. Specifically, these technologies can be used to collect large amounts of data about entire populations. These data can include race, ethnic group, gender, political affiliation, and socioeconomic status, which in turn can be used to stratify populations by demographics. Many of these demographics are sensitive and not necessarily related to a person's health, and might lead to stigmatisation of particular ethnic or socioeconomic groups.[21] Further, information such as racial demographics might lead to a surge in discrimination, as seen by a rise in attacks on people of southeast Asian descent in the COVID-19 crisis. Finally, stratifying populations on these grounds might reinforce existing divides that leave particular groups more vulnerable to the pandemic. Therefore, safeguards must exist for any digital public health technologies to prevent "the predictable from becoming exploitable".[32] Conversely, data collection should not be limited to epidemiological factors, but also capture socio-economic differences that are known to drive disparities in infection rates. Such efforts, especially when taking place in low-trust environments, need to be supplemented by robust safeguards, including analytical capacities to contextualise the data in order to avoid further stigmatisation of under-served populations and provide evidence-base for action against persistent health inequalities.[37]

Repurposing

There is a risk that digital tools could also be applied to other forms of surveillance in addition to being used for legitimate public health purposes (namely, tracking and monitoring patients with COVID-19). For example, a *New York Times* report investigated Health Code, an Alibaba-backed government-run application that supports decisions about who should be quarantined for COVID-19 in China. The report discovered that the application also appears to share information with the police.[38] Further, some countries have developed biosurveillance programmes that share some characteristics of both pandemic response and counter-terrorist programmes.[39] Therefore, it is crucial to distinguish digital public health technologies that allow third-party sharing of information for non-health-related purposes from those that do not.

Setting an expiration

Pandemics are a rare situation where democratic governments can take unchecked executive action decisions for the collective good of their population. These include actions that might be in contravention of political due process or individual human rights. If prolonged, these actions can deprive citizens of their rights, with no guarantee these rights will be restored after the end of the crisis. The USA Patriot Act, promulgated after the September 11 terrorist attacks in the USA, is a good example of how democratic liberties, such as the right to protection against warantless surveillance, might be ceded after an emergency. Likewise, there was an outcry after the Hungarian government led by Viktor Orban instituted powers by decree to fight the COVID-19 pandemic without an expiration date.[40] Therefore, heightened surveillance empowered by digital public health technologies should not continue after the COVID-19 pandemic has ended. Further, such programmes should clarify upfront the duration, what data they are collecting, and how long they will hold the information for.[41]

Preventing digital inequality

Digital technology, particularly mobile phone technology, is increasingly widespread globally but unevenly distributed. In 2019, two-thirds of the world's population did not own smart phone technology, and one-third did not own any mobile phone. Smart phone ownership disparities are particularly noticeable in emerging economies. For instance, in India, the world's second most populous country accounting for more than 17% of the global population, only 24% of adults report owning a smart phone.[42] Even in advanced economies with high smart phone ownership rates, not all age cohorts are catching up with digital tools. In 2018, most citizens of Japan, Italy, and Canada older than 50 years did not own a smart phone.[42] In addition, not all smart phones have the technology built in that is necessary to support certain functions, such as proximal location sensing.[43] Any digital public health technology solution that relies on mobile phones excludes those without access to these technologies for geographical, economic, or demographic reasons, as well as a broad range of already marginalised groups. If not complemented with non-digital strategies, the risk of exclusion of marginalised groups might exacerbate health inequalities.

When addressing these challenges, researchers and policy makers might face conflicts between different ethical values. In public health ethics, there is a continuing tension between public benefit and individual rights and civil liberties.[44] This tension mirrors an underlying conflict between personal autonomy (ie, protecting personal freedom) and beneficence (ie, maximising public benefit) and has already emerged in the ongoing COVID-19 pandemic as public-benefit-motivated lockdown measures have caused a temporary restriction to individual freedoms in the name of the public good. These include freedom of movement, freedom of assembly, and entrepreneurial freedom.[45] Digital public health technologies generate a similar tension with rights and freedoms, especially the rights to privacy and informational self-determination. Since these technologies require high uptake and massive and ubiquitous data availability to be effective, their successful deployment for the public good might conflict with the protection of private information of users (eg, their serological status, health records, geolocation, proximity, voice records, pedometrics and other activity data, data upload, and download transmission, etc). Risks for individual rights are also raised by a temporal factor—namely the urgent need to mitigate the pandemic. Software, application programming interfaces, and other digital tools require time to be developed in a privacy-preserving manner, and to be adequately validated via rigorous beta testing and pen testing. Given the immense time pressures under which global actors are operating, it is reasonable to expect that some of them will roll out tools without the necessary validation, and hence they won't be able to prevent misconfigurations, software bugs, and other errors that can jeopardise individual and collective privacy. To offset this risk of infringing individual rights, there must be a framework for deciding what public benefit is appropriate. In this regard, Laurie[46] suggests the test of reasonable benefit in the context of data sharing for pandemic response. Assessing what is reasonable for a digital public health technology depends on two main variables: scientific evidence and risk assessment. Prospective scientific evidence is necessary to predict and quantify the expected benefit of a new digital public health technology, and should be corroborated with the continuous monitoring of efficiency during the rollout phase. Risk impact assessments, including privacy impact assessment, are necessary to predict and quantify the potential risks, including risks for individual rights. Deployers of digital health technology have a moral responsibility to conform to the highest standards of scientific evidence and risk assessment, and show that the magnitude and probability of public benefit outweigh the magnitude and probability of risk at the individual level. In the absence of clear public health benefit, even minor restrictions of individual rights might result in being disproportional, and hence are unjustified. Whether one principle should be prioritised over another as a design choice is a matter that must be decided on a case by case basis and using established methods to resolve ethical conflicts or dilemmas such as risk–benefit assessment and reflective equilibrium. For example, among populations susceptible to COVID-19 (such as people older than 70), there might be lower computer literacy. Therefore, the beneficence principle might take priority over autonomy in justifying developing simplified digital public health technologies.

Ethical use of digital public health tools: a navigation aid

Decision makers (eg, researchers, technology companies, governments, and non-governmental organisations) who seek to embrace any of the emerging COVID-19 digital public health technologies have an obligation to address the ethical and legal challenges described in this article. To do so effectively, these decision makers need to translate the ethical–legal considerations into actionable safeguards that can unlock the promise of these technologies while avoiding harm and managing risks.

Best practices have not yet emerged for guiding the development and deployment of COVID-19 digital public health technologies specifically. Because the unique circumstances of this pandemic have triggered a rapid rollout of digital public health technologies, we propose a navigation aid to fill this gap. Our aid is founded on procedural values relevant to big data contexts—namely, accountability, consistency, engagement, reasonableness, reflexivity, transparency, and trustworthiness[47,48] Furthermore, this aid is built on general governance approaches frequently used in the context of risk mitigation and management at the intersection of digital technology and public policy that serve the goal to initiate and structure an analytical and, to the extent possible, inclusive deliberative process around risk (figure 3). The steps within this process include established mechanisms including privacy risk assessments, accountability schemes, and transparency measures.[49,50] The aim of the navigation aid is to provide immediate practical guidance by assisting involved decision makers to work towards a coherently structured and iterative process. This process can be deployed across the rapidly evolving spectrum of digital public health technologies to identify, assess, and manage the legal and ethical risks associated with these tools throughout their lifecycle.

Preparation phase

Firstly, this phase involves assembling the right team. The technical, organisational, legal, ethical, public health, and other challenges that need to be managed when using digital tools in response to COVID-19 are complex and require an interdisciplinary team. It is necessary to ensure a team from diverse backgrounds and ethnicity, with diverse experiences, and high integrity, that participate in communities of practice.[51]

Secondly, this phase requires the establishment of guiding ethical principles. In addition to ensuring compliance with fundamental rights and applicable legal norms, establishing clarity with respect to value commitments, red lines, and guiding principles will help to navigate tensions or conflicts between values when embracing digital technology against the fight of COVID-19. The set of principles (beneficence, justice, non-maleficence, privacy, solidarity, and autonomy) discussed in this article can serve as a reference point.[52–55]

Planning phase

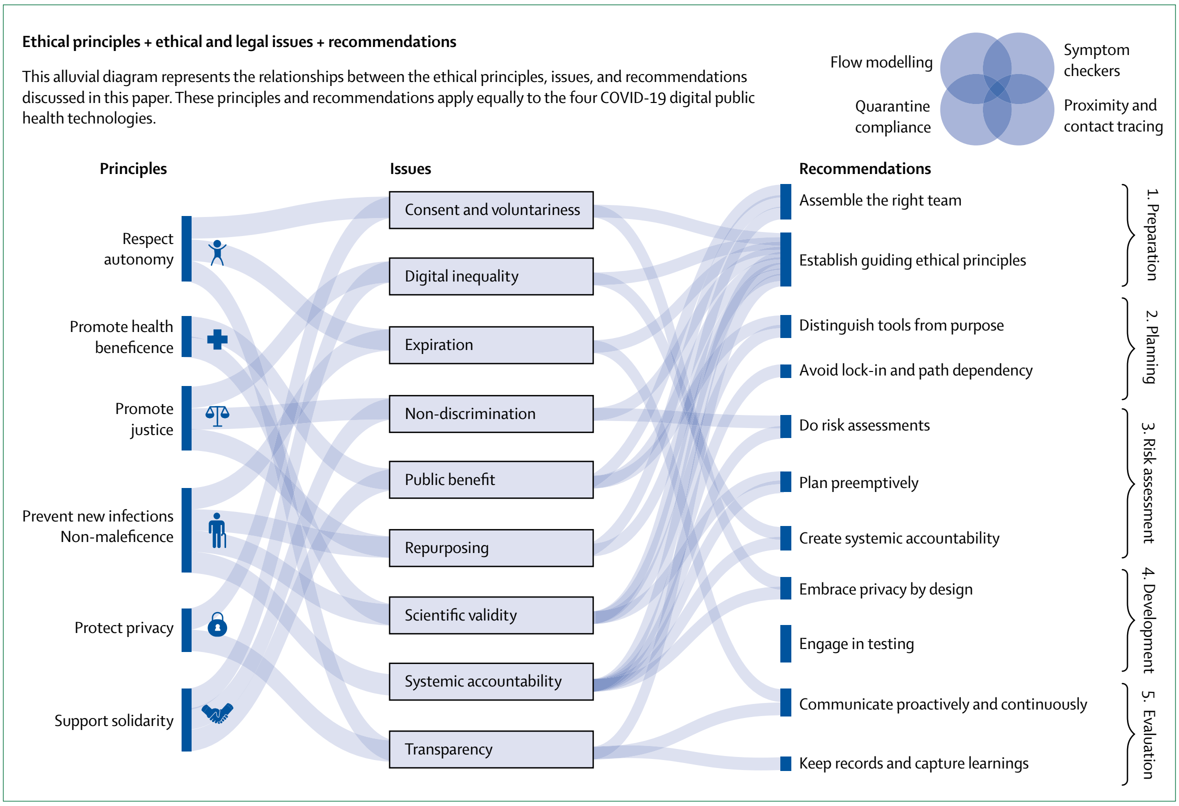
This phase entails distinguishing tools from their purpose. Defining specific objectives within the containment and mitigation strategy is necessary. Only then can the various digital public health technologies with their different data sources and means to collect, use, and otherwise process them, be considered.

Furthermore, this phase also includes avoiding lock-in and path dependency. With the use of the typology of public health technologies against COVID-19 offered in this Health Policy paper, the range of tools, techniques, and data governance models available once the questions and goals have been defined, should be considered. It is necessary to understand what the different instruments and models can and can't do, what their promise and limitations are, and use the aforementioned list of the technical, legal, and ethical core issues as evaluation criteria.

Assessment phase

For this phase, validation studies and risk assessments should be done. A robust and systematic risk assessment process should be done for each intended purpose, context, instrument, and model, even when pressed for time; well established practices such as human rights impact assessment and privacy risk impact assessment should lead the way, even if they need to be modified.[56] The assessment should not be limited to a question of compliance; a holistic ethics perspective should be applied, taking into account the substantive issues listed in the Mapping ethical and legal challenges part of this Health Policy paper.

Furthermore, preemptive planning should be done. The full lifecycle of data and systems should be considered and



Ethical principles + ethical and legal issues + recommendations

This alluvial diagram represents the relationships between the ethical principles, issues, and recommendations discussed in this paper. These principles and recommendations apply equally to the four COVID-19 digital public health technologies.

Figure 3: **Alluvial diagram representing the relationship between ethical principles, ethical and legal issues, and recommendations**

include both online and offline effects,[57] when conducting risk assessments and identifying appropriate safeguards. Special consideration is given because of context shifts over time and unintended consequences, second-order and third-order effects, and other similar factors. For example, although a proximity tracing tool might be privacy-preserving, identification might occur downstream when the person has to be isolated or quarantined.

Finally, it is necessary to create systemic accountability. Design and put into place mechanisms to monitor the development and deployment of digital public health tools, not only as a matter of compliance but also in terms of unanticipated ethical ramifications. Leverage existing institutional arrangements and processes and aim for independent, external oversight that brings together expertise from different fields to oversee the use of ethical health tools, develop stopping rules, and conduct period reviews. Following the systemic oversight framework, this accountability mechanism should be sufficiently adaptive, flexible, inclusive, and reflexive to account for the ever-evolving digital public health ecosystem.[48]

Development phase

This phase includes embracing privacy in so-called by design and by default approaches.[58] In terms of safeguards, this means considering and combining the most effective legal, organisational, and technical measures, including advanced statistical and computational safeguards to manage privacy and data protection risks and address ethical issues. Adopting privacy by design and by default principles from the outset, and building additional protective layers over time, are needed.

Additionally, this phase requires engaging in validation. Even under time pressure, the testing of software, application programming interfaces, and tools is crucial to avoid negative outcomes and violations of legal and ethical principles. With appropriate safeguards in place, it is necessary to team up with open-source communities, technical universities, and independent third-party laboratories to review components and systems.

Deployment and evaluation phase

First, this phase requires proactive and continuous communication. Transparency in the form of provocative communication with the key stakeholders—and where possible, active consultation and participation with the public—is essential and needs to be an integral part of the process from beginning to end. Establishing real-time feedback mechanisms during the deployment phase and evaluating the use and effect on an ongoing basis are necessary, making use of the goals set in the planning and selection phase as benchmarks and continuously updating risk assessment.

Second, this phase includes keeping records and capturing learnings. Throughout these steps, documentation is essential, both of the risk assessment itself and the safeguards and accountability mechanisms that have been taken to mitigate remaining risks, and serve as a basis for continued learning.

Limitations

There are three inherent limitations to our conclusions. The first is the technical limitations of the different types of applications described in this typology. The urgent nature of any pandemic means developers are under substantial time pressure to develop new software applications in response to changing evidence. However, a countervailing consideration is the reliability of both novel technologies in the time of a pandemic and the sources of the data. Specifically, complex technology not only takes a long time to develop, but is prone to failure, which in turn can undermine public trust and use of that technology.[59] Therefore, the technology and implementation strategies underlying digital public health technologies also contain notable ethical considerations. However, balancing which technical choices are preferable from an ethical perspective in granular detail is beyond the scope of this Health Policy paper. The second is digital public health technologies that might exist outside the typology that we describe in this paper. Specifically, our typology and ethical recommendations have been developed using software applications that are currently in existence. Therefore, the typology described in this article and the corresponding analyses are likely to evolve as new digital public health technologies designed for COVID-19 are emerging on an almost daily basis. Nonetheless, the functionalist character of our typology provides sufficient agility and flexibility to adapt to future and emerging technologies based on different software or hardware architectures compared with those available to date. Likewise, we do not address the use of artificial intelligence for pandemic management, as our Health Policy paper is focused on public health goals rather than technology types. Accordingly, we do not consider the large number of artificial intelligence ethics and governance principles that exist.[60] Further, we consider digital surveillance and contact tracing as part of a broader strategy that is conditioned on large-scale testing, universal access to health care, and adequate societal safety nets. The absence of these conditions results in the use of these digital tools being misguided and irresponsible, given the associated risks. Other technologies might be used to achieve different public health goals, such as mental health counselling for those in isolation and mutual aid for susceptible individuals. Although these technologies might not be used in disease diagnosis, they carry their own ethical considerations that should be considered by developers, public health agencies, and governments.[61] The third limitation pertains to managing competing ethical goals. In this paper, we do not engage with resolving the challenges we have identified. This engagement should be done in the context of specific technologies, health-care systems, and jurisdictions. Although this context is necessary and the subject of our ongoing research, we chose instead to focus on developing a principled aid to assist those called to resolve a multitude of ethical challenges. The use of the aid cannot guarantee the successful resolution of competing ethical goals in any given case, but it can ensure procedural robustness that is more likely to keep decision makers away from tragically wrong outcomes.

Conclusion

In the wake of the COVID-19 pandemic, there has been a surge in the development and deployment of digital public health technologies for pandemic management. However, these tools must be guaranteed to be scientifically and ethically sound to ensure widespread public trust and uptake. Typological analysis and established frameworks in public health and big data ethics can aid governments and other actors in discerning the complex ethical–legal landscape in which these digital tools will operate. By combining ethical–legal analysis with procedural considerations in technology governance, we propose a navigation aid which could help decision makers ensure procedural robustness and minimise ethical lapses when developing or deploying digital public health technologies. Given the magnitude of this pandemic and the ever-evolving nature of these technological solutions, the continuous monitoring and flexible adaptation of the aid to specific contexts might be required.

Contributors

UG and EV conceived of the article and developed the outline. UG, MI, JSc, JSl, and EV conducted the research and analysis. UG, MI, JSc, and EV drafted sections of the paper. JSl developed all graphics. All authors edited and revised the manuscript.

Declaration of interests

MI is partly funded by the Swiss National Science Foundation's National Research Programme 75 and the Swiss Academy of Medical Sciences (Käthe-Zingg-Schwichtenberg-Fonds 20/17). JSc is funded by the ETH Domain's Personalized Health and Related Technologies. All other authors declare no competing interests.

Acknowledgments

We thank Ryan Budish for providing constructive feedback on an earlier version of this manuscript which was circulated as a preprint.

References

1 Google. Apple and Google partner on COVID-19 contact tracing technology. April 10, 2020. https://blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/ (accessed April 11, 2020).

2 Ienca M, Vayena E. On the responsible use of digital data to tackle the COVID-19 pandemic. *Nat Med* 2020; **26:** 463–64.

3 Amnesty International. COVID-19, surveillance and the threat to your rights. April 3, 2020. https://www.amnesty.org/en/latest/news/2020/04/covid-19-surveillance-threat-to-your-rights/ (accessed April 10, 2020).

4 Gostin L. Public health strategies for pandemic influenza: ethics and the law. *JAMA* 2006; **295:** 1700–04.

5 Martin R, Conseil A, Longstaff A, et al. Pandemic influenza control in Europe and the constraints resulting from incoherent public health laws. *BMC Public Health* 2010; **10:** 532.

6 Laurie GT, Hunter KG. Mapping, assessing and improving legal preparedness for pandemic flu in the United Kingdom. *Med Law Int* 2009; **10:** 101–37.

7 Aghaizu A, Elam G, Ncube F, et al. Preventing the next 'SARS' - European healthcare workers' attitudes towards monitoring their health for the surveillance of newly emerging infections: qualitative study. *BMC Public Health* 2011; **11:** 541.

8 Lupton D. Beyond techno-utopia: critical approaches to digital health technologies. *Societies (Basel)* 2014; **4:** 706–11.

9 Collier D, Laporte J, Seawright J. Typologies: forming concepts and creating categorical variables. In: Box-Steffensmeier JM, Brady HE, Collier D, eds. The Oxford handbook of political methodology. Oxford: Oxford University Press, 2008: 153–68.

10 Cho H, Ippolito D, Yu YW. Contact tracing mobile apps for COVID-19: privacy considerations and related trade-offs. *arXiv* 2020; published online March 30. https://arxiv.org/abs/2003.11511 (preprint).

11 Berry AC. Online symptom checker applications: syndromic surveillance for international health. *Ochsner J* 2018; **18:** 298–99.

12 Drew DA, Nguyen LH, Steves CJ, et al. Rapid implementation of mobile technology for real-time epidemiology of COVID-19. *Science* 2020; published online May 5. https://doi.org.10.1126/science.abc0473.

13 Wang CJ, Ng CY, Brook RH. Response to COVID-19 in Taiwan: big data analytics, new technology, and proactive testing. *JAMA* 2020; **323:** 1341.

14 Buckee CO, Balsari S, Chan J, et al. Aggregated mobility data could help fight COVID-19. *Science* 2020; **368:** 145–46.

15 Findlay S, Palma S, Milne R. Coronavirus contact-tracing apps struggle to make an impact. May 18, 2020. https://www.ft.com/content/21e438a6-32f2-43b9-b843-61b819a427aa (accessed May 24, 2020).

16 Coughlin SS. How many principles for public health ethics? *Open Public Health J* 2008; **1:** 8–16.

17 Childress JF, Faden RR, Gaare RD, et al. Public health ethics: mapping the terrain. *J Law Med Ethics* 2002; **30:** 170–78.

18 Nebeker C, Bartlett Ellis RJ, Torous J. Development of a decision-making checklist tool to support technology selection in digital health research. *Transl Behav Med* 2019; ibz074.

19 Mello B, Wang C. Ethics and governance for digital disease surveillance. *Science* 2020; **368:** 951–54.

20 Roberts SL. Big data, algorithmic governmentality and the regulation of pandemic risk. *Eur J Risk Regul* 2019; **10:** 94–115.

21 Quinn P. Crisis communication in public health emergencies: the limits of 'legal control' and the risks for harmful outcomes in a digital age. *Life Sci Soc Policy* 2018; **14:** 4.

22 Hinch R, Probert W, Nurtay A, et al. Effective configurations of a digital contact tracing app: a report to NHSX. April 16, 2020. https://cdn.theconversation.com/static_files/files/1009/Report_-_Effective_App_Configurations.pdf?1587531217 (accessed June 25, 2020). University College London.

23 Hargittai E, Redmiles EM. Will Americans be willing to install COVID-19 tracking apps? April 28, 2020. https://blogs.scientificamerican.com/observations/will-americans-be-willing-to-install-covid-19-tracking-apps/ (accessed May 7, 2020).

24 Redmiles EM. User concerns & tradeoffs in technology-facilitated contact tracing. *arXiv* 2020; published online April 28. http://arxiv.org/abs/2004.13219 (preprint).

25 Nature. Show evidence that apps for COVID-19 contact-tracing are secure and effective. *Nature* 2020; **580:** 563.

26 London AJ, Kimmelman J. Against pandemic research exceptionalism. *Science* 2020; **368:** 476–77.

27 Yan SJ, Chughtai AA, Macintyre CR. Utility and potential of rapid epidemic intelligence from internet-based sources. *Int J Infect Dis* 2017; **63:** 77–87.

28 Ferretti L, Wymant C, Kendall M, et al. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science* 2020; **368:** eabb6936.

29 Servick K. Cellphone tracking could help stem the spread of coronavirus. Is privacy the price? March 22, 2020. https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price (accessed April 9, 2020).

30 Lee LM, Heilig CM, White A. Ethical justification for conducting public health surveillance without patient consent. *Am J Public Health* 2012; **102:** 38–44.

31 Wiewiórowski WR. Monitoring the spread of COVID-19. March 25, 2020. https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_covid-19_monitoring_of_spread_en.pdf (accessed May 17, 2020).

32 Garattini C, Raffle J, Aisyah DN, Sartain F, Kozlakidis Z. Big data analytics, infectious diseases and associated ethical impacts. *Philos Technol* 2019; **32:** 69–85.

33 Zanfir G. European Union's data-based policy against the pandemic, explained. April 30, 2020. https://fpf.org/2020/04/30/european-unions-data-based-policy-against-the-pandemic-explained/ (accessed May 5, 2020).

34 Kolfschooten HV. EU coordination of serious cross-border threats to health: the implications for protection of informed consent in national pandemic policies. *Eur J Risk Regul* 2019; **10:** 635–51.

35 Fingas J. India requires all workers to use its COVID-19 tracking app. May 3, 2020. https://www.engadget.com/india-requires-workers-to-use-covid-19-app-042811484.html (accessed May 6, 2020).

36 Hamilton IA. Poland made an app that forces coronavirus patients to take regular selfies to prove they're indoors or face a police visit. March 23, 2020. https://www.businessinsider.com/poland-app-coronavirus-patients-mandaotory-selfie-2020-3 (accessed April 9, 2020).

37 Chowkwanyun M, Reed Jr AL. Racial health disparities and Covid-19—caution and context. *N Engl J Med* 2020; published online May 6. https//:doi.org.10.1056/NEJMp2012910

38 Mozur P, Zhong R, Krolik A. In coronavirus fight, China gives citizens a color code, with red flags. March 1, 2020. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html (accessed April 9, 2020).

39 Kim AJ, Tak S. Implementation system of a biosurveillance system in the republic of Korea and its legal ramifications. *Health Secur* 2019; **17:** 462–67.

40 Bruszt L. Viktor Orban: Hungary's disease dictator. April 23, 2020. https://balkaninsight.com/2020/04/23/viktor-orban-hungarys-disease-dictator/ (accessed June 24, 2020).

41 Ng EST, Tambyah PA. The ethics of responding to a novel pandemic. *Ann Acad Med Singapore* 2011; **40:** 30–35.

42 Silver L. Smartphone ownership is growing rapidly around the world, but not always equally. Feb 5, 2019. https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/ (accessed April 9, 2020).

43 Bradshaw T. 2 billion phones cannot use Google and Apple contact-tracing tech. April 20, 2020. https://arstechnica.com/tech-policy/2020/04/2-billion-phones-cannot-use-google-and-apple-contract-tracing-tech/ (accessed May 5, 2020).

44 Bayer R. The continuing tensions between individual rights and public health. Talking Point on public health versus civil liberties. *EMBO Rep* 2007; **8:** 1099–103.

45 Nay O. Can a virus undermine human rights? *Lancet Public Health* 2020; **5:** e238–39.

46 Laurie GT. Cross-sectoral big data. *Asian Bioeth Rev* 2019; **11:** 327–39.

47 Laurie GT, Schaefer GO, Labude MK, et al. An ethics framework for big data in health and research. *Asian Bioeth Rev* 2019; **11:** 327–39.

48 Vayena E, Blasimme A. Health research with big data: time for systemic oversight. *J Law Med Ethics* 2018; **46:** 119–29.

49 Renn O, Klinke A. Risk governance and resilience: new approaches to cope with uncertainty and ambiguity. In: Fra Paleo U, ed. Risk governance: the articulation of hazard, politics and ecology. Dordrecht: Springer Netherlands, 2015: 19–41.

50 Organisation for Economic Co-operation and Development. Artificial intelligence in society. Paris: Organisation for Economic Co-operation and Development Publishing, 2019.

51 Ingram D, Ward J. Behind the global efforts to make a privacy-first coronavirus tracking app. April 7, 2020. https://www.nbcnews.com/tech/tech-news/behind-global-efforts-make-privacy-first-coronavirus-tracking-app-n1177871 (accessed April 11, 2020).

52 Jelinek A. Statement on the processing of personal data in the context of the COVID-19 outbreak. March 19, 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf (accessed April 11, 2020).

53 GSMA. The GSMA COVID-19 privacy guidelines. April, 2020. https://www.gsma.com/publicpolicy/wp-content/uploads/2020/04/The-GSMA-COVID-19-Privacy-Guidelines.pdf (accessed April 11, 2020).

54 Human Rights Watch. Joint Civil Society Statement: states use of digital surveillance technologies to fight pandemic must respect human rights. April 2, 2020. https://www.hrw.org/news/2020/04/02/joint-civil-society-statement-states-use-digital-surveillance-technologies-fight (accessed April 11, 2020).

55 Andrew J, Ramiro MA, Arnold BB, et al. NGO and expert statement to the OECD Secretary General on COVID-19, privacy and fundamental rights. April, 2020. https://www.apc.org/en/pubs/ngo-and-expert-statement-oecd-secretary-general-covid-19-privacy-and-fundamental-rights (accessed April 11, 2020).

56 Allison-Hope D, Vaughan J. COVID-19: a rapid human rights due diligence tool for companies. March 30, 2020. https://www.bsr.org/en/our-insights/blog-view/covid-19-a-rapid-human-rights-due-diligence-tool-for-companies (accessed April 11, 2020).

57 Altman M, Wood A, O'Brien DR, Gasser U. Practical approaches to big data privacy over time. *Int Data Priv Law* 2018; **8:** 29–51.

58 Greenwood D, Nadeau G, Tsormpatzoudi P, Wilson B, Saviano J, Pentland A. COVID-19 contact tracing privacy principles. April 6, 2020. https://law.mit.edu/pub/covid19contacttracingprivacyprinciples (accessed April 11, 2020).

59 Yasaka TM, Lehrich BM, Sahyouni R. Peer-to-peer contact tracing: development of a privacy-preserving smartphone app. *JMIR Mhealth Uhealth* 2020; **8:** e18936.

60 Jobin A, Ienca M, Vayena E. The global landscape of AI ethics guidelines. *Nat Mach Intell* 2019; **1:** 389–99.

61 Zhou X, Snoswell CL, Harding LE, et al. The role of telehealth in reducing the mental health burden from COVID-19. *Telemed J E Health* 2020; **26:** 377–79.