The Journal of Sociotechnical Critique

Volume 2
Issue 1 *Online First*

Article 1

April 2022

Public Goods From Private Data: An Effectiveness and Justification Dilemma for Digital Contact Tracing

Andrew Buzzell
York University, Toronto, abuzzell@yorku.ca

Recommended Citation

Buzzell, A. (2022). Public Goods From Private Data: An Effectiveness and Justification Dilemma for Digital Contact Tracing. *Journal of Sociotechnical Critique, 2*(1), 1-21. Advance online publication. https://doi.org/10.25779/zzja-hv81

Public Goods From Private Data: An Effectiveness and Justification Dilemma for Digital Contact Tracing

Cover Page Footnote

The author would like to thank Dr. Jay Shaw and Dr. Ross Upshur for helpful discussions of an earlier draft. This work was supported in part by funding from the Joint Centre for Bioethics at the University of Toronto and the Social Sciences and Humanities Research Council. The corresponding author states that there is no conflict of interest.

Public goods from private data: An effectiveness and justification dilemma for digital contact tracing

Andrew Buzzell
York University

Debate about the adoption of digital contact tracing (DCT) apps to control the spread of COVID-19 has focused on risks to individual privacy. This emphasis reveals significant challenges to ethical deployment of DCT, but generates constraints which undermine justification to implement DCT. It would be a mistake to view this result solely as the successful operation of ethical foresight analysis, preventing deployment of potentially harmful technology. Privacy-centric analysis treats data as private property, frames the relationship between individuals and governments as adversarial, entrenches technology platforms as gatekeepers, and supports a conception of emergency public health authority as limited by individual consent and considerable corporate influence that is in some tension with the more communitarian values that typically inform public health ethics. To overcome the barriers to ethical and effective DCT and develop infrastructure and policy that supports the realization of potential public benefits of digital technology, a public resource conception of aggregate data should be developed.

Keywords: privacy, AI ethics, big data, public health ethics, bioethics, paternalism, digital contact tracing

The debate about the adoption of digital contact tracing (DCT) apps to control the spread of COVID-19 has focused on risks to individual privacy (Sharma & Bashir, 2020; Tang, 2020). The first aim of this article is to show that this emphasis generates constraints which undermine justification to implement DCT. The second aim is to argue that it would be a mistake to view this result solely as the successful operation of ethical foresight analysis (Floridi & Strait, 2020) or anticipatory ethics, preventing deployment of potentially harmful technology. Privacy-centric analysis tends to implicitly adopt a private property model of data ownership, which frames the relationship between individuals and governments as adversarial, entrenches technology platforms as gatekeepers, and supports a conception of emergency public health authority as limited by individual consent and considerable corporate influence that is in some tension with the more communitarian values that typically inform public health ethics. To overcome the barriers to ethical and effective DCT and develop infrastructure and policy that supports the realization of potential public benefits of digital technology, a public resource conception of aggregate data should be developed.

Contact tracing and COVID-19

Since the successful development of contact tracing as a tool to help control diseases such as smallpox (Porco et al., 2004) and tuberculosis (Begun et al., 2013), public health authorities have had the power to compel individuals and organizations to provide data that can be used to analyze the movements and behaviour of an individual diagnosed with an infectious disease to identify possible incidents of transmission. Contact tracing allows public health authorities to identify potential transmission events and proactively attempt to limit further transmission with interventions such as isolation. When a person is diagnosed, a public health authority may interview them, ask for records such as transit and banking data, and then attempt to reconstruct possible contacts with other people that, given what is known about the disease, may have resulted in transmission. These people are in turn contacted, and depending on the nature of the specific disease, might be asked (or compelled) to undergo interview, examination, or even isolation. Manual contact tracing is time-consuming and treats individual data as a potential public resource, one for which access might be negotiated or appealed even when public health regulations might include powers to compel that data is provided. On the other hand, automated or digitized systems must treat this data as an always-on resource.

The virology of COVID-19 creates two kinds of scaling challenges that make manual contact tracing unfeasible. The mode of transmission is respiratory droplet spread, with some evidence of transmission via indirect surface contact (CDC, April 2021), and the potential for aerosolized transmission in some circumstances (Greenhalgh et al., 2021; Van Doremalen et al., 2020). With a reproductive rate sufficient for exponential case growth, this creates a horizontal problem of resource scale. In the US alone it is estimated that at least 100,000 full-time contact tracers would be required (Watson et al., 2020). The long period of incubation, and the period of asymptomatic transmission in particular, creates a vertical scaling problem where the amount of data required to conduct tracing for each individual is quite large, encompassing a 14-day period.

DCT apps could mitigate the vertical problem by assisting recall through recording high fidelity data for each individual that can be retroactively queried to identify potential transmission. DCT apps could also mitigate the horizontal problem by automating much of the contact tracing process (Ferretti et al., 2020). Even without a vaccine, an effective DCT program that correctly identifies transmission risks and mandates subsequent actions (that are publicly accepted and generally complied with) that prevent transmission could allow public authorities to relax some of the severe restrictions such as stay-at-home orders and business shutdowns

that have been imposed—an important counterfactual when considering the justifiability of DCT programs (Mello & Wang, 2020).

Most DCT proposals use Bluetooth Low Energy (BLE) radio networking technology present in smartphones and recording Received Signal Strength Indicator (RSSI) measurements to determine when devices are close together, and for how long. Unlike the tracking of GPS signals, which identify the location of a device geographically, RSSI signals only indicate that two devices have been in close range of one another. A database of device pairings and RSSI information is maintained on the device or a centralized server, and when one device is flagged as belonging to an infected individual, an algorithm can select from the database identifiers recorded while the individual may have been infectious, filter them by duration and signal strength, and produce a list of device IDs that might be targeted for intervention of some type, such as testing or self-isolation.

As a sociotechnical system, DCT re-taxonomizes RSSI data as predictions of disease transmission risk and recommends actions backed by public health authority. Justification for the ensuing actions depends in part on the reliability of the prediction. DCT faces serious effectiveness challenges with both prediction and coverage, summarized in the supplementary material. When the non-causal proxies for transmission are too weakly correlated with actual transmission risks, or the individual or population coverage is insufficient or uneven, DCT can't perform the function of identifying infection risks effectively. While predictive problems might be mitigated by improving technology and aggregating additional data, coverage problems threaten the viability of DCT directly, and are least amenable to post-hoc correction. They require populations be persuaded to use the DCT app, and that hardware and software vendors cooperate with public health authorities to resolve barriers to adoption and usage, such as the need for software modifications to enable passive RSSI measurement.

Effectiveness as a condition on justification

The exercise of coercive authority in the interests of public health is typically justified by the harm principle (Upshur, 2002): that the action is necessary to prevent harm to others. It is further limited by the principle of least infringement (Childress et al., 2002): that interventions which undermine privacy or autonomy must be the least burdensome alternative sufficient to support the public health objective that is independently justified by the harm principle. Effectiveness is therefore a necessary condition on justification, and any modulation of measures taken in response to other ethical concerns must maintain a level of effectiveness

consistent with claims that the intervention is a viable alternative (Allen & Selgelid, 2017). For example, evidence that the pervasive use of face coverings in public significantly reduces interhuman transmission of COVID-19 (Zhang et al., 2020) might justify the exercise of state power to make them compulsory—a limitation of autonomy, but one that is relatively low in costs and restrictions compared to alternatives such as mass shelter-at-home orders. The effectiveness of the less-restrictive alternative is high enough that the marginally better results from dramatically more severe restrictions are offset.

If responsiveness to ethical or legal requirements constrains implementation of DCT in ways that weaken its expected effectiveness, this in turn undermines justification for persuasive and coercive measures which aim to improve adoption. This might indicate a fundamental problem with the proposed intervention. Because the predictions made by DCT often trigger actions that further impact individual autonomy, such as quarantine, effectiveness is particularly critical. Moreover, because DCT has the potential to generate knowledge of risks that could save lives, decisions that dilute this epistemic capacity are themselves ethically salient (Dennett, 1986).

DCT and privacy

At a time of heightened public awareness of the privacy and security challenges presented by the ever-growing trail of data generated by our interactions with digital technologies (“data exhaust”), DCT has been subject to intense scrutiny on privacy grounds. There is a growing awareness that our data can be used in contexts that we would not consent to, and which could harm our interests. We might agree to let an app track our music listening habits to recommend playlists, but be dismayed to learn it can be used to make inferences about our mental health (Allen, 2015; Greenberg et al., 2016). Indeed, digital phenotyping of aggregate data from wide range of sources can generate health data and de-anonymize individuals. (Martinez-Martin et al., 2018; Sobhani, 2019).

Even where we might grant consent to use our data in one context of analysis, interpretation, and action, such as infectious disease control, we might not be able to foresee functions the data might be used for within it. Similar problems with informed consent arise in the context of genetic research (Lunshof et al., 2008), where uncertainty about usage problematizes consent, a problem magnified under the sociotechnical conditions in which digital data is collected and retained, which generates very little friction to such re-contextualization and re-taxonomization.

In light of these concerns, it is not surprising that many DCT models have focused on privacy-by-design with strict minimization of data collected and transmitted, strong anonymization, a prohibition of the use of additional data sources (such as GPS), and policies demanding regular deletion of data and restrictions on uploading data to central servers. Privacy-preserving DCT models have been extremely influential, as evidenced by the extent to which implementations have coalesced around privacy-preserving standards (Chan et al., 2020; Li & Guo, 2020; Tang, 2020) such as MIT's Private Kit (MIT, 2020), PEPP-PT (PEPP Team, 2020) and DP-3T (Troncoso et al., 2020), and the extent to which technology platform providers and health institutions (World Health Organization, 2020) have embraced this approach.

The exposure notification API as a theory of public health authority power

Because the design of mobile operating systems prevents the passive collection of Bluetooth data, the cooperation of vendors is necessary to build effective DCT apps. The dominant mobile operating system vendors, Apple and Google, jointly and rapidly developed the "Exposure Notification API" (Apple & Google, 2020) to support limited DCT capabilities. This was released as an update to mobile operating systems in order to afford development of Bluetooth RSSI based DCT. Access to the Exposure Application Programming Interface (API) is tightly controlled, and only one app can be deployed in a country. The vendors can disable and remove the app at any time. The app cannot use any data source except Bluetooth RSSI data obtained via the Exposure API. The app cannot transmit this data to a central server. The Exposure API provides a methodology for the calculation of disease transmission risk which public health authorities configure by setting some pre-defined values.

The structure of the Exposure API expresses and enforces a policy perspective on the relationship between public health authorities and citizens who use the products manufactured by Apple and Google. This treats data as private property, frames the relationship between individuals and governments as adversarial, entrenches technology platforms as gatekeepers and offers a conception of emergency public health authority as limited by individual consent and considerable corporate influence. This is an unconventional view—historically, privacy is not a significant constraint on manual contact tracing, and even strong legislation such as HIPAA recognizes the legitimate need for public health authorities to access protected health information (HIPAA 45 CFR 164.512)

Technology companies require a great deal of public trust to operate, as do governments and public health authorities. Because of the need for

cooperation with governments to build DCT, vendors are exposed to highly publicized risks in the deployment of DCT, in terms of maintaining trust and also in avoiding additional regulation. The privacy-preserving model serves vendor interests, allowing them to cooperate with public health authorities, thus avoiding regulatory or coercive measures by limiting the possibility that the use of DCT apps breaks tacit or contractual agreements with their users that could damage already wavering public trust. (Newton, 2020).

Privacy-preserving DCT constrains solutions to effectiveness problems

Critically, the Exposure Notification API prevents several actions that might be undertaken to improve the effectiveness of DCT. Coverage problems that relate to contexts where smartphone ownership or physical possession is uneven could be partially remediated by aggregating other data, as could the predictive weaknesses of RSSI. Including additional data, such as location, would help avoid common scenarios where exposures are repeatedly registered at testing sites, requiring further testing leading to subsequent further exposure notifications. Several so-called “super-spreader” events have occurred in contexts where physical possession of the device is unlikely, such as choir practices (Hammer, 2020). Analysis of the data exhaust surrounding such events could indicate the transmission risks, even where Bluetooth radio proximity would not.

However, this is also an example of a case where the possibility of accurate and highly personal inferences from latent information in our data raises fears of surveillance and concerns about how the access to aggregate data could lead to personal harms. There are important questions about who might be afforded access to such data, how this would be controlled, and how its use can be confined to justified purposes. While there are good reasons to fear that data could accidentally or intentionally become available to be used for purposes which are harmful, it’s valuable to consider the causes of these fears. There is a risk of a “whiplash effect” (Mittelstadt & Floridi, 2016) where policy overreacts to perceived risks of harms. But that there is a perception of risk (however justified) is also a policy failure—that technology companies have not been held to higher standards of accountability and trustworthiness has created an atmosphere in which technological opportunities to pursue public health objectives are foreclosed.

The aggregation of data, including GPS, on central servers where it can be subject to further analysis and enrichment might also improve the epidemiological value of DCT (Mello & Wang, 2020). Some countries have

political, demographic, and cultural characteristics that might favour the use of multiple apps, and data preservation may have future epidemiological value.

If privacy-maximizing constraints on DCT undermine effectiveness, this in turn can weaken justification to deploy DCT at all. One might conclude that this is the correct outcome of ethical analysis of DCT: that it cannot be used ethically because requirements needed to generate the effectiveness required for public health objectives are unjustifiably invasive or coercive.

Alternately, one might wonder if this suggests that privacy-maximizing analysis is problematic. It is somewhat dismaying that a public health intervention that we have the technical means to deploy, which would be a much less restrictive alternative to measures currently in effect, becomes unjustifiable because of the restrictions necessary to ensure minimization of privacy risks. In particular, the Exposure API's restrictions on upload to central servers for further analysis and the collection of GPS data—both measures adopted to increase privacy—foreclose opportunities to enrich DCT data in ways that could help to address effectiveness problems.

Concerns about security and mission creep are only accidentally supportive of privacy maximization. While there are legitimate reasons to think that the sociotechnical infrastructure DCT apps depend on are too insecure to trust, these are generally not inherent but are instead the results of implementation decisions. In practice, we are able to mitigate these problems to support many sensitive applications. There will be many examples of poorly implemented DCT, such as Qatar's which leaked personal data in QR-codes (Amnesty International UK, 2020), but this does not mean that secure DCT is not possible.

One might also worry that governments will misuse the data down the road, but emergency public health legislation enacted in most jurisdictions have strict limitations that we should trust to function as intended. Even if we have upstream worries about the rule of law in some jurisdiction, this is a distal problem, and not one that weighs in favour of the privacy-maximizing view generally. In addition to legal constraints, the introduction of citizen monitoring would help address these concerns, such as the practice of co-determination in Germany, for example, where works councils have the right to examine and oversee the usage of any equipment that can be used to monitor workers (Gürtler & Höffler, 2005).

A prediction and coverage dilemma

The problem of effective coverage is one of trust and influence as much as it is technical: adequate coverage and compliance depends in part on

the public's willingness to cooperate. Discussion of DCT dominated by privacy and security concerns and messaging that prioritizes the protection of individual privacy both influence public opinion, shaping the conditions of consent, which in turn affects the extent of coercive measures necessary to encourage adoption of DCT. Some jurisdictions plan to use choice architecture, such as defaulted opt-in, to encourage adoption and avoid coverage problems, but choice architecture and the theory of libertarian paternalism that underlies it depend on the absence of strong preferences (Sunstein, 2015), and preferences can be shifted by the exercise of soft power in the information environment. Because the extent of the coercion is itself part of the justification calculus, changes in public sentiment can impact justification.

An example of this relation between sentiment and justification is the effectiveness of anti-vaccination information operations (Johnson et al., 2020; McKee & Middleton, 2019; Wang et al., 2019) which lead to a reduction in vaccine compliance in many jurisdictions, some of which have responded by increasing coercive regulation. This would be a difficult response to enact or justify if a majority of the population did not support it. Anti-vaccination propaganda is often produced and amplified by state and non-state actors that do not aim to improve epistemic outcomes, and often intend or are ambivalent to harms caused directly and indirectly, and this propaganda exists alongside and sometimes displaces the sincere expression of concerns and hesitations by genuine discourse participants. It can be particularly dangerous when it erodes a democratic mandate for the very actions that would mitigate the damage, such as state-backed evidenced-based messaging.

The dilemma which arises for DCT is that increasing privacy protection in order to overcome constraints on justification undermines predictive effectiveness to an extent that weakens justification to deploy DCT at all. But to relax these protections to improve predictive effectiveness conflicts with public sentiment (Milsom et al., 2020), creating resistance to adoption that would exacerbate coverage problems, again weakening justification on effectiveness grounds, but also increasing the justificatory burden because implementation against public sentiment raises the stakes in terms of autonomy impingement.

The remainder of this article explores a route to resolve this dilemma by examining the conditions that make the privacy objections so difficult to overcome.

Communitarian bioethics, principlist technology ethics

Public sentiment against impingements on privacy necessary for DCT is grounded in legitimate fears of pervasive security problems with the

sociotechnical infrastructure. The litany of security and privacy problems with DCT applications that have already been deployed (Privacy International, 2020) reinforce this. Even apps compliant with the Exposure Notification API have been found to share data with other apps on the phone (Reardon, 2021).

However, this sentiment is also shaped by an increasingly prominent public discussion of technology ethics that is framed in a way that sits uneasily alongside the values that inform public health ethics. A dominant strain of technology ethics, exemplified by legal expressions such as the EU's GDPR and California's CCPA as well as many AI ethics charters and codes of conduct (Jobin & Vayena 2019), resembles a format in bioethics that came to be known as "principlism" (Beauchamp & Childress 2001, Clouser & Gert 1990). This is the view that a minimal set of principles, usually autonomy, non-maleficence, beneficence, and justice, supply the analytical machinery needed to approach ethical problems. It is criticized on the grounds that it does not specify an ordering, which instead is often inherited from the context of application, which tends to privilege the liberal individualist emphasis on autonomy, and which is unable to fully articulate principles such as beneficence beyond self-interest. (Callahan, 2003). Applied technology ethics tends to generate trade-off dilemmas, such as that between innovation and precaution, or between privacy and public goods. As with principlism in bioethics, it does not supply a decision procedure for conflict resolution. This is particularly challenging when institutions that produce technological artefacts and systems struggle with "...onboarding external ethical perspectives..." (Metcalf & Moss, 2019) that conflict with tacit and explicit internal norms. Our underlying moral interest in applied ethics demands more than compromise and consilience. Rather, as Callahan puts it: "[s]erious ethics, the kind that causes trouble to comfortable lives, wants to know what counts as a good choice and what counts as a bad choice" (Callahan, 2003).

A primary criticism of principlism has been the extent to which it privileges autonomy and individual choice—an explicit motivation in the germinal work of Beauchamp and Childress. They criticized the “beneficence-based model of health care ethics..” and aimed to shift it “in the direction of an autonomy model, while also incorporating a wider set of social concerns, particularly those focused on social justice” (Beauchamp, 2007). This motivation stemmed in part from recognition that a great deal of ethical problems in the health care context involve a lack of respect for individual autonomy, such as the failure to allow patients to refuse treatment. Callahan, even while critiquing the central role of autonomy, observes that a virtue of principlism is that it is “culture congenial” with the individualistic culture in which it emerged (Callahan, 2003). One problem with the foregrounding of autonomy is that it comes into tension with the desire to remain responsive to social justice concerns when these arise in contexts

where balances must be found between individualistic goods and community or population goods.

What's particularly interesting in the context of building public health interventions from big data is the extent to which concerns about effectiveness and justice expose limitations of the autonomy-centric ethical frame at a structural level. The institutional entities (mostly private corporations) which capture, store, process, and apply big data sets occupy positions of power that are inextricably bound up with a private-property model of data. Individuals in some limited sense "own" their data, and grant custodianship to these entities in exchange for benefits they value such as applications. This supports a "demand-as-blame" (Supran & Oreskes, 2021) account of corporate action, paradigmatically illustrated by the ways in which the tobacco and fossil fuel industries offer a framing of their activities as merely responding to consumer demand, obscuring from view the conditions that shape and generate this demand, and supporting a narrative that prohibits "fundamental social change that would disrupt the fossil fuel industry" (Smerecnik & Renegar, 2010). Likewise, the sociotechnical imaginary of big data is one where the private-property frame is implicit. Consumers demand that tech platforms collect and shield their data from government, which creates structural barriers to the realization of the potential of these data sets to promote public goods. Privacy-first discourse has a tendency to embed this framing, obscuring ways of thinking about aggregate data in ways that transcend the private ownership model.

The "communitarian turn" in bioethics arose in part because capabilities emerging in genetic research created opportunities for public goods that could only be ethically realized once focus on individual interests yielded to more communitarian principles such as solidarity and public benefit. (Chadwick, 2011). Predictive genetic analysis that might benefit an individual, their family, and their community—now and in the future—exposes information that might be prejudicial to the individual's interests, such as by interfering with their ability to acquire health insurance (Fulda & Lykens, 2006; Launis, 2003). The extended value of genetic data over long timelines and across unforeseeable applications problematizes the coherence and applicability of autonomy protections such as informed consent. An ethical framework that could motivate policy and regulation to enable the pursuit of these opportunities for public good required the integration of communitarian values.

The use of big data sets to power analytical technologies or to train AI systems introduces similar concerns. Inability to detect and account for bias and noise in data can cause the resulting technologies to operate in ways that are unreliable, unfair, or ineffective. For example, a neural network trained to perform diagnosis of diabetic retinopathy in a laboratory

with high accuracy was unreliable in clinical applications: many patients underwent imaging with equipment that lacked the high fidelity of the images used in the training data (Gulshan et al., 2016), causing the model to perform unreliably depending on where patients were located.

Technologies built with AI and big data are highly sensitive to the extent to which data reliably represents the community where it will be deployed, which generates bioethical concerns that are characteristically communitarian in a way that is distinctive when compared to conventional medical technology. The performance of AI technology can vary across differing segments of the population in which it might be used and can produce harms that cannot be predicted in advance. For example, a widely deployed medical screening algorithm was found to systematically underestimate the health risks of black patients because the algorithm used future costs as a proxy for risk, and due to existing inequities, black populations would be allocated fewer resources (Obermeyer et al., 2019).

Public health ethics introduces consideration of solidarity, proportionality, and reciprocity alongside the four core principles of biomedical ethics (Coughlin, 2014; Lee, 2012; Schröder-Bäck et al., 2014). The inclusion of communitarian perspectives is necessary because policies and interventions that support public health objectives by the very nature of their concern with population-level goods can impose costs and burdens on individuals that do not directly benefit them, which can expose the limits of individualistic analysis that privileges autonomy. Communitarian and distributive considerations could help resolve some of the ordering problems principlist technology ethics inherits from the liberal individualist context it operates within, which would help to resolve tradeoffs by giving greater weight to shared values and common goods.

A public resource approach

If DCT cannot be deployed in a way that is ethical and effective, this is an unfortunate loss of a public health opportunity. The barriers to remediation run deeper than privacy-preserving technical measures and stem from the need to develop a conception of aggregate personal data as a public resource. We lack critical legal, policy, and technical infrastructure to realize an alternate sociotechnical imaginary where the data exhaust from our increasingly instrumented and networked activities can be fairly and safely used in the public interest.

The Exposure Notification API encodes and enforces a privacy and autonomy maximizing model of DCT, essentially privatizing a public health policy concern. One justification for this is that corporations are enabling their users to protect their personal property or adhering to a contractual

obligation (Taddeo & Floridi, 2016). Traditional contact tracing treats our personal data as a potential public resource with synchronous consent and access procedures triggered by the identification of transmission risk, whereas DCT treats it as a de facto public resource with always-on consent and access. DCT provides public benefits based on data collected from many individuals who might never have an elevated risk. Its value is at the population level, and we would accept impingement on our privacy for the good of the community. Although privacy is usually regarded as a paradigmatically individual concern, communitarian approaches to privacy (O'Hara, 2010; Floridi, 2017) argue that groups can have privacy rights, and that privacy is fundamentally a common good where its value and limits are in reciprocal tension with other community values.

Technology companies profit from the value they extract from aggregate data, which depends on pervasive access to individual data in ways that have resulted in compromises of user privacy. Aggregate data is exponentially more economically and informationally valuable than that of individuals; it confers significant soft power to influence public sentiment and hard power in terms of material control of data. But it is not clear that the equivocation between personal data as the private property of an individual, and aggregate data as the private property of the collector, is justified. Napoli (2019) argues that "whatever the exact nature of one's individual property rights in one's user data may be, when these data are aggregated across millions of users, their fundamental character changes in such a way that they are best conceptualized as a public resource." If aggregate data is substantially and uniquely distinctive, this supports the application of public trust doctrine, which is based on the idea that "because of their unique characteristics, certain natural resources and systems are held in trust by the sovereign on behalf of the citizens" (Calabrese 2001), such as the protection of public lands and waters. In some jurisdictions, public trust doctrine has been used to support claims that the state is liable for inactivity and inattention in protecting public resources from new and existing threats (British Columbia v. Canadian Forest Products Ltd., 2004). Public trust doctrine applied to data as a public resource would require the development of strategy and infrastructure that could proactively protect this resource in the public interest.

The exploration of a more communitarian approach to applied technology ethics and the articulation and assertion of a public resource rationale applicable to the data we generate by engaging with digital technology and services could enable policy and regulation that would directly address the barriers I have argued stand in the way of effective and ethical DCT. Where policy and legislation such as the GDPR, especially through the Data Protection Impact Assessment (DPIA) process, identifies

and protects risks to individual interests, methodologies to identify and protect opportunities in the public interest lag behind. Articulating an alternative to the private-property model of data ownership and control is an enabling condition for the realization of opportunities to use aggregate data for public good and would act as a check on the centralization of decisive power over public policy in the hands of multinational technology corporations.

Supplementary material: DCT's effectiveness challenges

Inherent effectiveness challenges

The virology of COVID-19, so far as it is understood, makes the re-taxonomization of Bluetooth RSSI data as COVID-19 exposure risks problematic because the mode of transmission and infectivity is such that there is only a weak likelihood that any particular contact detected by DCT results in transmission, whereas for diseases such as tuberculosis or HIV/AIDS, it is easier to identify exposure events with high transmission probability. The contact/transmission link is also problematic due to the potential for transmission via indirect surface contact.

Reliance on smartphones

There are socioeconomic confounders related to smartphone ownership and use that will skew representation and the ability to install and update DCT apps. Life patterns in some populations generate periods of contact with others when smartphones are not present. Some forms of employment generate a large number of contacts with others, which may or may not actually correspond to increased risks of transmission. Evidence for non-nosocomial transmission in Japan shows primary cases in several contexts where smartphones are frequently not on persons or are turned off, such as at music events and gyms (Furuse et al., 2020).

Bluetooth RSSI as a proxy for exposure

There are effectiveness problems with the core technology. RSSI measurements map only weakly to transmission risk, because BLE radio signals travel through walls and barriers used in public spaces to specifically to prevent droplet spread. RSSI is stronger when we walk side-by-side rather than following one another. It is weakened when phones are in pockets or while sitting around a table, and is sensitive to many idiosyncratic features of indoor environments (Leith & Farrell, 2020). There are also considerable differences in RSSI measurement for different devices and different mobile operating systems (BlueTrace, 2020), which introduces socio-economic confounds.

Security

Effectiveness can be further undermined by deliberate exploitation of security vulnerabilities (Vaudenay, 2020). The public health value of DCT is undermined by even simple circumventions, such as the display of screen captures instead of running apps, as has been observed in India with mandatory Aarogya Setu app (Clarence, 2020).

Individual and population coverage

At the population level, DCT apps would have to be in use by 60% of a population (Servick, 2020) to be effective. This challenge led Singapore to consider making their app mandatory, but the proposal was later abandoned due to implementation challenges (Mahmud, 2020). Various jurisdictions have considered opt-in, opt-out, and incentivization schemes to encourage uptake.

At the individual level, coverage involves the extent of the individual's activities and behaviours that are accurately captured by the DCT app. Aside from issues related to smartphone ownership and presence described above, mobile phone operating systems place limits on the ways apps can access Bluetooth radios, often requiring apps be open and in use. Even an individual who has installed the app and has their phone at all times would produce little useful DCT data in this case. This problem is in fact a critical barrier to effective DCT and requires the cooperation of operating system vendors to remediate. Requiring users to keep their phones open and the apps on-screen is not viable.

References

Allen Anderson, P. (2015). Neo-muzak and the business of mood. *Critical Inquiry, 41*(4), 811–840.

Allen, T., & Selgelid, M. J. (2017). Necessity and least infringement conditions in public health ethics. *Medicine, Health Care and Philosophy, 20*(4), 525–535. https://doi.org/10.1007/s11019-017-9775-0

Amnesty International UK. (2020, May 26). *Qatar: 'huge' security weakness in COVID-19 contact-tracing app.* Amnesty International UK. https://www.amnesty.org.uk/press-releases/qatar-huge-security-weakness-covid-19-contact-tracing-app

Apple Inc. and Google Inc. (2020) *Exposure notifications: Help slow the spread of COVID-19, with one step on your phone.* Google. https://www.google.com/covid19/exposurenotifications/

Begun, M., Newall, A. T., Marks, G. B., & Wood, J. G. (2013). Contact tracing of tuberculosis: A systematic review of transmission modelling studies. *PLoS One, 8*(9), e72470. https://doi.org/10.1371/journal.pone.0072470

Beauchamp, T. L., & Childress, J. F. (2001). *Principles of biomedical ethics.* Oxford University Press.

Beauchamp, T. L. (2007). The 'four principles' approach to health care ethics. *Principles of Health Care Ethics*, 3–10.

BlueTrace. (2020). *Trial Methodologies.* GitHub. https://github.com/opentrace-community/opentrace-calibration/blob/master/Trial%20Methodologies.md

British Columbia v. Canadian Forest Products Ltd., (2004) 2 S.C.R. 74, 2004 SCC 38.

Callahan, D. (2003). Principlism and communitarianism. *Journal of Medical Ethics, 29*(5), 287–291. https://dx.doi.org/10.1136%2Fjme.29.5.287

Centers for Disease Control and Prevention. (2021, April 5). *SARS-CoV-2 and surface (Fomite) transmission for indoor community environments.* Centers for Disease Control and Prevention. https://www.cdc.gov/coronavirus/2019-ncov/more/science-and-research/surface-transmission.html

Chan, J., Cox, L.P., Foster, D., Gollakota, S., Horvitz, E., Jaeger, J., Kakade, S., Kohno, T., Langford, J., Larson, J., Sharma, P., Singanamalla, S., Sunshine, J., & Tessaro, S. (2020). PACT: Privacy sensitive protocols and mechanisms for mobile contact tracing. *Bulletin of the IEEE Computer Society Technical Committee on Data Engineering,* 43(2), 15–35.

Chadwick, R. (2011). The communitarian turn: myth or reality?. *Cambridge Quarterly of Healthcare Ethics, 20*(4), 546–553. https://doi.org/10.1017/S0963180111000284

Childress, J. F., Faden, R. R., Gaare, R. D., Gostin, L. O., Kahn, J., Bonnie, R. J., Kass, N., Mastroianni, A.C., Moreno, J., & Nieburg, P. (2002). Public health ethics: mapping the terrain. *The Journal of Law, Medicine & Ethics, 30*(2), 170–178. https://doi.org/10.1111/j.1748-720x.2002.tb00384.x

Clarence, A. (2020, May 15). Aarogya Setu: Why India's Covid-19 contact tracing app is controversial. *BBC News.* From https://www.bbc.com/news/world-asia-india-52659520

Clouser, K. D., & Gert, B. (1990). A critique of principlism. *The Journal of Medicine and Philosophy, 15*(2), 219–236. https://doi.org/10.1093/jmp/15.2.219

Coughlin, S. S. (2008). How many principles for public health ethics? *Open Public Health Journal, 1*, 8–16. https://dx.doi.org/10.2174%2F1874944500801010008

Dennett, D. C. (1986). Information, technology, and the virtues of ignorance*. Daedalus*, 135–153.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bosnall, D., & Fraser, C. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science, 368,* (6491). https://doi.org/10.1126/science.abb6936

Floridi, L. (2017). Group privacy: A defence and an interpretation. In L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group Privacy* (pp. 83–100). Springer.

Floridi, L., & Strait, A. (2020). Ethical foresight analysis: What it is and why it is needed?. *Minds and Machines, 30*, 77–97. https://doi.org/10.1007/s11023-020-09521-y

Fulda, K. G., & Lykens, K. (2006). Ethical issues in predictive genetic testing: A public health perspective. *Journal of Medical Ethics, 32*(3), 143–147. https://dx.doi.org/10.1136%2Fjme.2004.010272

Furuse, Y., Sando, E., Tsuchiya, N., Miyahara, R., Yasuda, I., Ko, Y. K., Saito, M., Morimoto, K., Imamura, T., Shobugawa, Y., Nagata, S., Jindai, K., Imamura, T., Sunagawa, T., Suzuki, M., Nishiura, H., & Oshitani, H. (2020). Clusters of coronavirus disease in communities, Japan, January-April 2020. *Emerging Infectious Diseases, 26*(9), 2176–2179. https://dx.doi.org/10.3201%2Feid2609.202272

Greenberg, D. M., Kosinski, M., Stillwell, D. J., Monteiro, B. L., Levitin, D. J., & Rentfrow, P. J. (2016). The song is you: Preferences for musical attribute dimensions reflect personality. *Social Psychological and Personality Science, 7*(6), 597–605. https://psycnet.apa.org/doi/10.1177/1948550616641473

Greenhalgh, T., Jimenez, J. L., Prather, K. A., Tufekci, Z., Fisman, D., & Schooley, R. (2021). Ten scientific reasons in support of airborne transmission of SARS-CoV-2. *The Lancet, 397*(10285), 1603–1605. https://doi.org/10.1016/S0140-6736(21)00869-2

Gürtler, O., & Höffler, F. (2015). Monitoring of workers and product market competition: The role of works councils. *Economic Inquiry, 53*(2), 136–-1379. https://doi.org/10.1111/ecin.12182

Hamner, L., Dubbel, P., Capron, I., Ross, A., Jordan, A., Lee, J., Lynn, J., Ball, A., Narwal, S., Russell, S., Patrick, & D., Leibrand, H. (2020). High SARS-CoV-2 attack rate following exposure at a choir practice—Skagit County, Washington, March 2020. *CDC Morbiity and Morality Weekly Report (MMWR), 69*(19), 606–610. http://dx.doi.org/10.15585/mmwr.mm6919e6

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence, 1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Johnson, N. F., Velásquez, N., Restrepo, N. J., Leahy, R., Gabriel, N., El Oud, S., Zheng, M., Manrique, P., Wuchty, S., & Lupu, Y. (2020). The online competition between pro-and anti-vaccination views. *Nature, 582*, 230–233. https://doi.org/10.1038/s41586-020-2281-1

Launis, V. (2003). Solidarity, genetic discrimination, and insurance: A defense of weak genetic exceptionalism. *Social Theory and Practice, 29*(1), 87–111. https://doi.org/10.5840/soctheorpract20032914

Leith, D. J., & Farrell, S. (2020). Coronavirus contact tracing: Evaluating the potential of using Bluetooth received signal strength for proximity detection. *ACM SIGCOMM Computer Communication Review, 50*(4), 66–74.

Li, J., & Guo, X. (2020). COVID-19 contact-tracing apps: A survey on the global deployment and challenges. https://arxiv.org/abs/2005.03599

Lee, L. M. (2012). Public health ethics theory: Review and path to convergence. *Journal of Law, Medicine & Ethics, 40*(1), 85–98. https://doi.org/10.1111/j.1748-720x.2012.00648.x

Lunshof, J. E., Chadwick, R., Vorhaus, D. B., & Church, G. M. (2008). From genetic privacy to open consent. *Nature Reviews Genetics, 9*(5), 406–411. https://doi.org/10.1038/nrg2360

Martinez-Martin, N., Insel, T. R., Dagum, P., Greely, H. T., & Cho, M. K. (2018). Data mining for health: Staking out the ethical territory of digital phenotyping. *npj Digital Medicine, 1*(1), 1–5. https://doi.org/10.1038/s41746-018-0075-8

Mahmud, A. H. (2020, June 5). COVID-19: Govt developing wearable contact tracing device, may be distributed to everyone in Singapore. *CNA,* from https://www.channelnewsasia.com/news/singapore/covid-19-contact-tracing-device-trace-together-app-12806842

McKee, M., & Middleton, J. (2019). Information wars: Tackling the threat from disinformation on vaccines. *BMJ, 365* (l2144). https://doi.org/10.1136/bmj.l2144

Mello, M. M., & Wang, C. J. (2020). Ethics and governance for digital disease surveillance. *Science, 368*(6494), 951–954. https://doi.org/10.1126/science.abb9045

Metcalf, J., & Moss, E. (2019). Owning ethics: Corporate logics, Silicon Valley, and the institutionalization of ethics. *Social Research: An International Quarterly, 86*(2), 449–476, from https://datasociety.net/wp-content/uploads/2019/09/Owning-Ethics-PDF-version-2.pdf

Milsom, L., Abeler, J., Altmann, S. M., Toussaert, S., Zillessen, H., & Blasone, R. P. (2020, May 12). Survey of acceptability of app-based contact tracing in the UK, US, France, Germany and Italy. *Center for Open Science*. osf.io/7vgq9

Mittelstadt, B. D., & Floridi, L. (2016). The ethics of big data: Current and foreseeable issues in biomedical contexts. *Science and Engineering Ethics, 22*(2), 303–341. https://doi.org/10.1007/s11948-015-9652-2

Morley, J., Cowls, J., Taddeo, M., & Floridi, L. (2020). Ethical guidelines for COVID-19 tracing apps. *Nature, 582* (7810), 29–31. https://doi.org/10.1038/d41586-020-01578-0.

Newton, C. (2020, March 2). The Verge tech survey. *The Verge.* https://www.theverge.com/2020/3/2/21144680/verge-tech-survey-2020-trust-privacy-security-facebook-amazon-google-apple

Napoli, P. M. (2019). User data as public resource: Implications for social media regulation. *Policy & Internet, 11*(4), 439–459. https://doi.org/10.1002/poi3.216

O'Hara, K. (2010). Intimacy 2.0: Privacy rights and privacy responsibilities on the world wide web. *University of Southampton Institutional Repository.* http://eprints.soton.ac.uk/268760/

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science, 366*(6464), 447–453. https://doi.org/10.1126/science.aax2342

PEPP-PT (2020) Pan-European privacy-preserving proximity tracing. *PEPP-PT.* https://web.archive.org/web/20200409221119/https://www.pepp-pt.org/

Porco, T. C., Holbrook, K. A., Fernyak, S. E., Portnoy, D. L., Reiter, R., & Aragón, T. J. (2004). Logistics of community smallpox control through contact tracing and ring vaccination: A stochastic network model. *BMC Public Health, 4*(1), 34. https://doi.org/10.1186/1471-2458-4-34

Privacy International. (2020). Apps and Covid-19. *Privacy International*. https://privacyinternational.org/examples/apps-and-covid-19

Reardon, J. (2021, April 27). Why Google should stop logging contact-tracing data. *AppCensus Blog.* https://blog.appcensus.io/2021/04/27/why-google-should-stop-logging-contact-tracing-data/

Schröder-Bäck, P., Duncan, P., Sherlaw, W., Brall, C., & Czabanowska, K. (2014). Teaching seven principles for public health ethics: Towards a curriculum for a short course on ethics in public health programmes. *BMC Medical Ethics, 15*(1), 73. https://doi.org/10.1186/1472-6939-15-73

Servick, K. (2020, May 21). COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work?. *Science*. https://www.science.org/content/article/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how

Sharma, T., & Bashir, M. (2020). Use of apps in the COVID-19 response and the loss of privacy protection. *Nature Medicine, 26*, 1165-1167. https://www.nature.com/articles/s41591-020-0928-y

Sobhani, M. (2019). HIPAA isn't enough: All our data is health data. *USC Center for Body Computing.* https://www.uscbodycomputing.org/uncensored/hipaaisnotenough

Sunstein, C. R. (2015). The ethics of nudging. *Yale Journal on Regulation, 32*(2). 413–450. https://digitalcommons.law.yale.edu/yjreg/vol32/iss2/6/.

Taddeo, M., & Floridi, L. (2016). The debate on the moral responsibilities of online service providers. *Science and Engineering Ethics, 22*(6), 1575–1603. https://doi.org/10.1007/s11948-015-9734-1

Tang, Q. (2020). Privacy-preserving contact tracing: Current solutions and open questions. https://arxiv.org/abs/2004.06818

Troncoso, C., Payer, M., Hubaux, J. P., Salathé, M., Larus, J., Lueks, W., Stadler, T., Pyrgelis, A., Antonioli, D., Barman, L., Chatel, S., Patterson, K., Čapkun, S., Basin, D., Beutel, J., Jackson, D., Roeschlin, M., Leu, P. Preneel, B., … Pereira. J. (2020). Decentralized privacy-preserving proximity tracing. *IEEE Data Engineering Bulletin, 42*(2), 36–66.

Upshur, R. E. (2002). Principles for the justification of public health intervention. *Canadian Journal of Public Health, 93*(2), 101–103. https://doi.org/10.1007/bf03404547

Van Doremalen, N., Bushmaker, T., Morris, D. H., Holbrook, M. G., Gamble, A., Williamson, B. N., Tamin, A., Harcourt, J. L., Thornburg, N. J., Gerber, S. I., Lloyd-Smith, J. O., de Wit, E., & Munster, V.J. (2020). Aerosol and surface stability of SARS-CoV-2 as compared with SARS-CoV-1. *New England Journal of Medicine, 382*(16), 1564–1567. https://doi.org/10.1056/nejmc2004973

Vaudenay, Serge (2020). Analysis of DP3T Between Scylla and Charybdis Cryptology ePrint Archive: Report 2020/399. IACR. http://eprint.iacr.org/2020/399

Wang, Y., McKee, M., Torbica, A., & Stuckler, D. (2019). Systematic literature review on the spread of health-related misinformation on social media. *Social Science & Medicine*, *240*(112552), 1–12. https://doi.org/10.1016/j.socscimed.2019.112552

Watson, C., Cicero, A., Blumenstock, J., & Fraser, M. (2020). A national plan to enable comprehensive COVID-19 case finding and contact

tracing in the US. *Johns Hopkins Bloomberg School of Public Health, Center for Health Security.* https://www.centerforhealthsecurity.org/our-work/pubs_archive/pubs-pdfs/2020/200410-national-plan-to-contact-tracing.pdf

World Health Organization. (2020, May 28). Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing. *World Health Organization.* https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

Zhang, R., Li, Y., Zhang, A. L., Wang, Y., & Molina, M. J. (2020). Identifying airborne transmission as the dominant route for the spread of COVID-19. *Proceedings of the National Academy of Sciences*. *117*(26), 14857–14863. https://doi.org/10.1073/pnas.2009637117