CASE STUDY

Is there a moral obligation to install the “COVID Alert SA” contact-tracing app on your phone?

Introduction

Contact-tracing app ("CTA") technology raises questions that are typically studied in the 'ethics of risk imposition', because it raises a conflict of moral interests that potentially poses a risk to people, to the harm they wish to avoid and to the values they wish to protect. Central in the study of the ethics of risk imposition is the question "When is it morally acceptable for one party to impose a new risk on another, or to permit the continuance of an avoidable situation which imposes risks" (Hayenhjelm, Wolff, 2012).

The conflict of interests raised by CTA technology is motivated by the risk of harm that results from the clash of two intuitively opposing and mutually exclusive moral obligations: the moral obligation to contribute to, or at least not obstruct human collective wellbeing, *versus* the moral obligation to protect people's individual privacy and autonomy.

Sharing personal information by means of CTA technology may pose a risk to the individual user's privacy, while refusing to use the CTA may pose a risk to society's collective efforts to curb the spread of the global COVID-19 pandemic. I will in what follows analyse and evaluate both claims, and attempt to reconcile the deontological rights and duties these claims imply with the harmful and beneficial consequences they (may) cause, in an attempt to formulate a reasonable compromise as justification for why everyone that can afford it ought to contribute to CTA technology.

1. DESCRIBE

We live in what has been coined the ‘information society’ - a society powered and controlled by massive streams of digital data-based information, relentlessly collected from interconnected people and technologies, aggregated, analysed, evaluated, shared and traded, and fed back into other technologies that drive an increasing amount of personal and social decision-making processes. “We can no longer unplug our world from ICTs[1] without turning it off” (Floridi 2014, 168).

It is not surprising then, that an important part of our current efforts to manage the COVID-19 pandemic, is fundamentally relying on technology - from collecting and disseminating information about the pandemic to the medical hospital equipment used to treat patients and the development and distribution of vaccines. While all of these technologies and their applications raise morally controversial concerns[2] which fall outside the scope of this case study, we will in what follows focus on one of these technologies and its moral controversies: the contact-tracing app (CTA).

In addition to news and information, a risk-assessment tool and COVID-19 test results made available by the South African National Department of Health via WhatsApp or SMS as part of its COVIDConnect programme, a mobile application was launched on 1 September 2020: the ‘COVID Alert SA app’.

Contact-tracing technology is a modern, ICT-based, automated application of a well established[3] medical practice of ‘contact-tracing’, whereby people that have

[1] Information and Communication Technologies

[2] including conspiracy and fake news dissemination, fair distribution of vaccines and specialised medical technology in hospitals, and new and largely untested technologies used in the development of vaccines.

[3] See for example theconversation.com/contact-tracing-how-physicians-used-it-500-years-ago-to-control-the-bubonic-plague-139248 and en.wikipedia.org/wiki/Contact_tracing

been in recent close proximity of a person that tests positive for a contagious disease are notified of the risk of having contracted the disease, and requested to monitor symptoms and quarantine to prevent the disease from spreading any further. Technological automation of the contact-tracing process is beneficial in two ways: it takes out the need for a call centre or health professional to manually, case by case, contact people that have found themselves in close proximity of an infected person, and it relieves people of the difficult task of accurately remembering who they have been in close proximity with in recent weeks - ICTs have no problem to keep a record of this information.

The COVID Alert SA app, developed by Discovery's software team for the South African National Department of Health, is free to download and built on the 'Exposure Notifications' Application Programming Interface (API) that Google and Apple have jointly made available on their respective mobile platforms. Data to use the app has been zero-rated by all of South Africa's mobile network providers. The app is powered by 'Bluetooth', a wireless technology standard that has been in use since 1989 for exchanging data between devices over short distances using ultra high frequency radio waves.[4] Bluetooth-enabled devices constantly 'listen' for other bluetooth-enabled devices nearby, while at the same time broadcasting their own presence to other devices in close range. When two devices equipped with the COVID Alert SA app are within two metres of each other for more than 15 minutes, random, regularly updated numerical codes, as well as the date, the proximity of the devices (based on signal strength) and the duration of proximity is exchanged between the devices.

The identity and location of the device users are not collected or used, and not needed for the CTA technology to work successfully. The random codes

[4] Bluetooth is managed by the Bluetooth Special Interest Group (SIG), and manufacturers must meet Bluetooth SIG standards to market it as a Bluetooth device (Wikipedia)

exchanged between devices are stored on each device for sixteen days. Should an app user test positive for COVID−19, the COVID Alert SA app allows him or her to voluntarily and anonymously report this information to the app community. This sets in motion the automated contact-tracing process. *Firstly*, the mobile device uploads the random codes that it has on record from the past sixteen days to the central Exposure Notification Server. *Secondly*, the Server sends these random codes to all other app users, whose device will run through these random codes to check for a match between these codes and the codes it has itself stored in the past sixteen days every time it has come into contact with another device equipped with the COVID Alert SA app. If there is a match, the device will notify its user of the possibility that she or he has been exposed to COVID−19, and of the date of the exposure, symptoms to look out for and measures to adhere to.

2. DISCERN

CTA technology raises a number of controversial moral issues. While one issue raises its moral head in the shape of a classic moral dilemma, another issue is known in the study of ethics as a ‘collective action problem’. I will in what follows in this current chapter delve deeper into the questions these issues raise, and attempt to provide answers to the questions in Chapter 3 below.

2.1. Risk as a moral dilemma

CTA technology relies on, and is powered by data that is collected from individual people - or to be more accurate: from individual people’s mobile devices. The ethical controversy is motivated by the clash of two intuitively opposing moral obligations, typically known as a ‘moral dilemma’, or the moral necessity to

choose between two opposing, mutually exclusive moral obligations: the moral obligation to contribute, or at the very least not obstruct, the collective fight against the COVID-19 pandemic *versus* the moral obligation to respect and protect each and everyone's individual autonomy, liberty and personal safety by means of protecting everyone's privacy. Applied to our case at hand, while the former moral obligation can be met by installing and using CTA technology, the latter can be met by refusing to share personal information via ICTs like CTA technology. A crucial question in our attempt to reconcile both moral obligations is whether or not CTA technology requires personal information to function efficiently.

CTA technology potentially poses a risk to its users' privacy, but not using the CTA potentially poses a risk to the efficiency of the collective fight against COVID-19. Broadly speaking, questions of risk may be ethically analysed and evaluated by two approaches: the cost-benefit analysis, and the deontological rights-based approach. While the former attempts to resolve questions of risk by means of probability calculations of harm and benefits based on empirical evidence, the latter requires a moral evaluation and rational justification of opposing moral rights and duties. The question we're left with is: how to choose between two opposing, mutually exclusive moral obligations?

2.2. Risk as a collective action problem

CTA technology raises questions that share characteristics with a classic moral problem known as a 'collective action problem'. There are many situations in which all members of a group benefit from efforts contributed by other members, or by all members collectively. But the incentive to contribute an individual effort may be questioned, seeing that one individual's contribution hardly makes any noticeable difference, or indeed no difference at all - known as the "argument

from inconsequentialism" (Sandberg, 2011). People that benefit from others' contributions, but themselves do not make any contribution, are known as 'free riders'.

A pandemic is a collective action problem, because it can only be overcome by collective contributions by all members of society. As we will see in the next chapter, CTA technology only works if enough people contribute data. However, it may seem that an individual's action - be it the wearing of a face mask, keeping social distance, consenting to vaccination, or indeed using the CTA - hardly makes any difference in the global fight against the pandemic. This is a problem, because "… the short-term self-interest of individual actors is in conflict with the longer-term collective interests, generating a substantial risk that the collective benefit is not produced at all" (Olson, 1965 in Jagers, S.C., Harring, N., Löfgren, Å. et al., 2020). So we find ourselves faced with the question: why should anyone make the effort of using the CTA, seeing that individual contributions hardly make a difference in the global fight against COVID-19?

2.3. Risk as an interplay between moral agents

Central in Sven Ove Hansson's 'Ethical Risk Analysis' (Hansson, 2018) is the identification and differentiation of three parties that play particular roles, or combinations of roles in relation to one another, in any situation of risk: people that bear the (possible) costs, people that reap the (possible) benefits and people that are in a position to decide whether or not the risk is taken or allowed to continue. In the case of what we may call 'individualism', all three roles are taken up by one and the same party. In the case of 'paternalism', one party decides, but another party reaps the benefits or suffers the cost - depending on how the risky situation unfolds. 'Maternalism' allows for one party to be in charge of the decision on whether the risk is taken or allowed to continue and to bear any

possible costs, while if there turns out to be a benefit to be reaped, it will be reaped by another party. In the case of 'externalities' the party that reaps the possible benefits is also in charge of the decision, while another party bears any costs that may occur. Finally, 'adjudication' defines a risky situation directly opposed to individualism: all three roles are distributed among three different parties.

Applied to our case at hand, we may distinguish the following parties and roles in the 'risky situation' that is caused by CTA technology. *Firstly*, only the South African government is in a position to decide which technology should power the CTA, and whether the CTA should be compulsory or voluntary for all citizens. For the government to decide (as they have) that the CTA is voluntary and powered by anonymous Bluetooth technology[5] creates a risk in terms of South Africa's efficiency in the fight against COVID-19 - it may result in later detections of and slower response to cluster outbreaks - but steers clear from imposing a potential involuntary risk to citizens' privacy. We may add that in making the CTA voluntary, government shifts the moral responsibility of CTA usage to individual citizens.

Secondly, South African citizens are not in a position to decide about who should participate or which technology should power the CTA, but they are in a position to decide for themselves whether or not to make use of the app and thereby contributing to the collective fight against COVID-19. South African citizens may further be distinguished in CTA users on the one hand, and CTA non-users, made up of CTA sceptics that refuse to use the app for various reasons, and people that cannot use the app, because they do not own a smartphone[6] on the other hand.

---

[5] and not by more accurate, personally identifiable data like names, ID numbers, geolocation and face recognition

[6] Only 35% of South Africans owns a smartphone.
Source : statista.com/statistics/625448/smartphone-user-penetration-in-south-africa/

Thirdly, recurring problems - arguably the main problems - in the debate about the protection of privacy, is the fact that harm is not necessarily caused by the direct exchange of personal information between a data subject and a data processor, but by third parties and by what is known as "function creep". Third parties can be anyone that has an interest in having access to large sets of personal data, whether that interest is social, economic, or political. The astronomical value of personal data on global brokerage markets and advertising bidding platforms is an indication of how many people, companies and governments share this interest.[7] "Function creep" is the usage and application of information (often by third parties) for a different purpose than for what it had been collected and consented to initially, often with invasions of privacy as a result. A classic example is tracking employee check-in and check-out times by means of the workplace secure access system, or using email addresses collected via a website's login system to send out direct marketing messages.

This leaves us with four distinct parties - the government, CTA users, CTA non-users, and (potential, unidentified) third parties - that interact in the context of two distinct risks - the risk of slowing down efforts to fight a pandemic and thereby infecting avoidable numbers of people, and the risk to CTA users's privacy. To return to Hansson's terminology, we may say that:-

* government unilaterally decides (and is morally responsible for), *firstly* not making the CTA compulsory (thereby potentially hampering the collective fight against COVID-19), and *secondly* to build the CTA on possibly inaccurate and inefficient Bluetooth technology (more about this later);
* individual citizens take up the role of decision-makers (and morally responsible agents) by voluntarily deciding whether or not to use the CTA;

[7] For example: Sales of location-targeted advertising based on personal geo-location data is estimated at US$ 21 billion per year by BIA Advisory Services, a "recognized authority for data-centered research, analysis, consulting and valuations for the [US] media industry." biakelsey.com. A good reference for definitions and explanations of geo-location may be found at quadrant.io

* potential harm in respect of privacy is only shared by CTA users, while they share in the collective benefits CTA technology potentially generates;
* CTA ‘sceptics’ (who can, but refuse to use the CTA) are ‘free riders’;
* the harms that result from not using CTA technology, or from using inefficient CTA technology, and the benefits that result from efficient use of CTA technology, are shared by all South Africa’s citizens;
* government and (potential, unidentified) third parties benefit in two ways: an efficient fight against COVID-19 results in lower public healthcare expenses and a faster economic relaunch, and data collected from large numbers of people are (commercially and politically) highly valuable on the global data brokerage markets.

It is clear then that all decision-makers share in the potential harms and benefits, albeit different harms and benefits, while (potential, unidentified) third parties only share in benefits. While this is not a pure case of ‘adjudication’, I believe it is the theoretic model that comes closest to describing the risk resulting from CTA technology.

3. DETERMINE

We may attempt to resolve the moral dilemma, the collective action problem and the complex interplay between moral agents postulated in Chapter 2 by *firstly* looking at empirical evidence for harms and benefits resulting from CTA technology, *secondly* by weighing up reasonable justifications for or against the right to privacy, *thirdly* by arguing for how an individual contribution to CTA technology may have a real impact on collective health, and *fourthly* by looking at how the moral views on privacy of modern, liberal and democratic majorities are reflected in current legislation. My conclusion is an attempt to pull together and reconcile all of the above in a reasonable, practicable compromise.

3.1. Resolving the moral dilemma

3.1.1. Consequentialism: Fact-based prediction of risk

We may calculate the probability of risk based on a cost-benefit analysis of the facts. The facts about potential costs to privacy are clear: Bluetooth-based CTA technology *does not* collect personal, identifiable information. In other words, the CTA does not pose a factual risk to people's privacy.[8]

But what about the benefits? Whether or not the Bluetooth-based CTA delivers the anticipated benefits depends on a number of facts that may be verified on the basis of empirical evidence - evidence, however, that is currently sketchy and hard to come by. Let's look at the available evidence.

[8] The distrust that may exist among the public with regard to big tech companies and governments who have shown a blatant disregard for privacy in the past, should not undermine the facts: it is factually, technically impossible to identity a person from the anonymous exchange of random codes. Whether the codes would enable re-identification in future, either by linking the codes to identifiable information, or by means of new technology, is at this point not a foreseeable and reasonable risk.

There is empirical evidence from models and real-life cases for the claim that CTA technology contributes to curbing the spread of a pandemic, and that the more people contribute to the CTA network, the more infections may be prevented. Using a simulation model, researchers Almagor and Picascia demonstrated that "… smartphone-based contact-tracing is a viable epidemic mitigation strategy, worth pursuing on the part of governments. The model suggests that, as larger fractions of society adopt the CTA, the spread of the virus is increasingly reduced, and, therefore, the benefits extend to the wider population. In principle, the CTA offers speed and cost efficiencies that can complement and extend traditional manual contact-tracing methods."[9]

Real-life cases of successful CTA technology can be found in China, Singapore, Israel, Poland and South Korea[10] which "utilised a centralised system that scrutinised patients' movements, identified people who had been in contact with patients, and used apps to monitor people under quarantine." [11]

CTA technology requires a population that owns a smartphone capable of downloading and running the app. For South Africa, this applies to 35% of the population.[12] Given the number of people that actually own a smartphone, the technology only works if it has been adopted by a sufficient percentage of the population. Across the world, the adoption rates appear to be generally low, with Australia at the top with 21.6%.[13] For South Africa, the only publicly available figures date back to 13 October "… the COVID Alert SA app (…) has been

[9] nature.com/articles/s41598-020-79000-y

[10] newyorker.com/news/news-desk/seouls-radical-experiment-in-digital-contact-tracing

[11] spectrum.ieee.org/biomedical/devices/contact-tracing-apps-struggle-to-be-both-effective-and-private

[12] statista.com/statistics/625448/smartphone-user-penetration-in-south-africa/

[13] statista.com/statistics/1134669/share-populations-adopted-covid-contact-tracing-apps-countries/

downloaded by 600,000 people in South Africa"[14], 22 September 2020 "More than half a million South Africans have now downloaded the Covid-19 tracing app"[15] and 4 December 2020 "COVID-19 alert app notches up 1m downloads."[16]

Oxford researchers have, by means of the 'epidemiological model' they have developed, concluded that " … we need around 56% of the total population to use the app to completely suppress the epidemic, if combined with 'shielding' of over 70s. Usage requirement may be lower if the app is used in conjunction with further social distancing interventions."[17] In addition, contact-tracing apps need "adequate political backing" and must be "properly integrated into public-health systems" to be efficient.[18] This same consideration - the need to integrate CTA technology into existing health care systems - had already been been made in 2015 by researchers in the fight against Ebola in Guinea: "When the decision is made to implement technology, it is critical to accompany the deployment with close managerial oversight to quickly correct data inconsistencies and to address challenges."[19]

Of course, adoption rates cannot only be based on download figures of the app, but should include app users' willingness to actually report a positive test and adhere to measures of isolation in case of a positive notification. While it may be possible to digitally measure the number of downloads and device interactions, it is unclear how people's actual, behavioural interactions with the app can be measured.

---

[14] dailymaverick.co.za/article/2020-10-13-covid-alert-sa-app-the-fine-balance-between-public-health-privacy-and-the-power-of-the-people/

[15] businessinsider.co.za/half-a-million-south-africans-download-the-covid-tracing-app-2020-9

[16] itweb.co.za/content/WnpNgq2KJn1vVrGd

[17] research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown

[18] nature.com/articles/d41586-021-00451-y

[19] ncbi.nlm.nih.gov/pmc/articles/PMC4682588/

3.1.2. Deontology: Moral evaluation of risk

From a deontological, rights-based moral perspective, risk may be defined as a potential infringement of values, duties and rights we deem important and wish to protect. In the case of CTA technology, two of these values are at stake: the collaborative effort to protect humanity against a pandemic, and the individual right to protection of privacy.

Of course, the possibility of infringing on values alone cannot suffice to categorically object to any action that may cause infringement. Almost every action has an impact on, and poses a risk to other people and their values. Zero-risk-tolerance would simply paralyse society. Our right not to be exposed to risk is therefore a "defeasible right" (Hansson, 2013) - we accept reasonable justifications to defeat it.

Privacy is a value we wish to protect, but, as we will see later in the discussion of current legislation, privacy is not an absolute right - we do accept conditions that call for its suspension. A deontological evaluation of CTA technology therefore requires a balancing act between different, often opposing values - a balancing act that is best performed by weighing up rational arguments in an attempt to formulate a reasonable compromise.

3.1.2.1. Arguments for privacy

1. Privacy protects autonomy. Modern liberal societies are built on the principles of the individual liberty and autonomy of their citizens, and because these principles are so intrinsically interwoven in the very fabric of our societies, they deserve robust protection. We see this protection in founding charters all over the liberal world (which I discuss later).

2. If knowledge is power, then the protection of privacy prevents that too much power is given to people and institutions we may not agree with, or that may try to control and manipulate us, and predict our behaviour for commercial and political purposes (Veliz, 2020).
3. 'Informational privacy' is a particular kind of privacy that aims to protect personal information that constitutes individual identities. An essential aspect of a person's individual autonomy is deciding which information about that person may be shared or published. Informational privacy has been given new meaning and at the same time come under increased threat in recent decades with the global advent of ICTs, which rely on big data streams of personal information. This has lead many governments around the world,[20] including South Africa, to step up the legal protection of their citizens against unwanted collection, storage, usage, sharing and publication of private information.
4. Privacy is something we deeply value and something we deem intrinsically human. Privacy is "social currency" - the sharing of intimacy and secrets reinforce social bonds (Cullison, 2018).
5. It is not contradictory to claim individual autonomy on the one hand, and protect people against negative applications and consequences of that autonomy. The information society has created a "… heavily skewed, asymmetric relationship between those that data is collected from, and those that reap the benefits from data processing. There is a 'big data divide' (Andrejevic, in Richterich 2018, 39) among stakeholders in data processing. "A modern understanding of justice requires that we protect the weakest party in an asymmetric relationship. The less agency people have in deciding whether or not they consent to sharing personal information, the higher the protection that is morally required. Involuntarily, unknowingly

[20] For this case study most notably the European Union's General Data Protection Regulation (2018) and South Africa's Protection of Personal Information Act (2013)

shared information deserves the highest possible protection" (Seynhaeve, 2020).

6. Privacy protection is not only a personal matter. Each and everyone has a social duty to protect his or her private information, because any information one person shares may have consequences for other individuals that belong to the same genetic, social, economic, political, ethnic or cultural group. Because big data analysis allows for the detection of behavioural patterns that may be ascribed to particular groups of people, these patterns may potentially be used to predict, control and manipulate people's behaviour. The Cambridge Analytica scandal[21] is a good example of how sharing personal information may have an impact of social and political dimensions.
7. Privacy protects personal safety. A New York Times investigation[22] found that a test subject's precise but anonymous geolocation data was recorded by 75 companies 8,600 times over a period of four months - on average, once every 21 minutes. This implies that once this data has been collected it may be shared with numerous (scrupulous and less scrupulous) companies anywhere in the world, for any kinds of purposes. As the New York Times points out, "Businesses say their interest is in the patterns, not the identities, that the data reveals about consumers. They note that the information apps collect is tied not to someone's name or phone number but to a unique ID." But the question is not what is currently and knowingly done with the raw data, but what can be done, or what can be done with new technologies in the future. Anyone with access to raw location data can easily consult public records to find out who lives at a particular location that they have tracked anonymously. As a matter of fact, researchers have already demonstrated in 2013 that "human

[21] In 2018, Cambridge Analytica was exposed for having used the personal data of up to 87 million Facebook users, harvested via a Facebook app called *This Is Your Digital Life*, in the manipulation of online commercial and political campaigns.

[22] Valentino-Devries J., Singer N., Keller MH and Krolik A (2018) *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret.* The New York Times. Available at nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [Accessed 25 March 2021]

mobility traces are highly unique" and therefore seemingly anonymous geo-location data can be re-identified when aggregated with known personal information like home address, work and school address: "… four spatio-temporal points are enough to uniquely identify 95% of the individuals" (de Montjoye, YA., Hidalgo, C., Verleysen, M. et al., 2013).

3.2.1.2. Arguments against privacy

1. The concept of privacy - its object and justifications - is blurred. While a 'reductionist interpretation' of privacy (Floridi 2014) tries to argue that societies and people would be worse off without privacy, an 'ownership-based interpretation' makes the claim that privacy is an individual, natural and inalienable right. But both interpretations are open to critique: on the one hand, we can think of positive consequences of a society without privacy too, in which crimes that currently escape prosecution, and unfair economic competition based on secret knowledge monopolies, would be a thing of the past. How privacy is valued, is relative, not absolute. There is no 'value of privacy in itself', there is nothing inherently and universally 'human' about privacy. It is valued differently in different circumstances. People freely exchange privacy for services or goods they desire. It is valued differently in public spaces than in our homes, over time, across cultures, social positions and even among different individuals (Seynhaeve, 2020).
2. If privacy aims to protect autonomy and freedom, what exactly are autonomy and freedom, and do they exist? If privacy aims to protect individual identities, exactly what are these identities, and are they as free and autonomous as we like to tell ourselves?
3. There are demonstrable, utilitarian benefits generated by suspending privacy in favour of social cooperation, of which CTA technology is a clear example. But there are other examples of "good data" (Gilbert, 2021) too. Sharing and

aggregating large amounts of personal information reveals new insights into human behaviour, while prioritising privacy over and above other fundamental rights can obstruct efforts to detect, expose and prosecute injustice in the world.

4. The right to privacy is not absolute. It is a historically developed legal concept with roots in Western liberalism, that must be applied relative to the overall function it was given in the context of other fundamental rights. The right to privacy can be suspended in favour of other reasonably justified concerns and priorities (more about this below).
5. Why are people particularly concerned about CTA privacy violations while they seem so utterly unconcerned about other privacy violations? To motivate CTA hesitance by privacy concerns seems inconsistent with the current ubiquitous "confessional culture" (DeBrabander, 2020) in which so many people voluntarily, consensually and openly share very private information with all kinds of ICTs - including social media, location-based applications and customer memberships. Recent research at The Trinity College Dublin exposed that Google and Apple "… devices not only collected data about handset activity, but also about handsets nearby; when a user connects to a wifi network the WiFi MAC addresses of other devices on the network are sent to Apple. The WiFi MAC address identifies a device on a WiFi network and so, for example, uniquely identifies your home router, cafe hotspot or office network. That means Apple can potentially track which people you are near to, as well as when and where."[23]

[23] irishtimes.com/business/technology/smartphones-share-our-data-every-four-and-a-half-minutes-says-study-1.4521267

3.2. Resolving the collective action problem

Why would anyone contribute to CTA technology, what difference does it make? *Firstly*, we have shown above that CTA technology depends on collective action - the more people contribute data to the CTA, the more efficient the technology is at preventing and containing cluster infection outbreaks.

Secondly, because a CTA functions as an early warning system of an individual infection to the rest of society, any individual's contribution may have a real collective impact. One's decision to quarantine after receiving an app notification, or one's notification to the app community of a positive corona test, is in a very real way able to prevent further infections and save lives.

Thirdly, it is to everyone's benefit to overcome COVID-19 as quickly as possible. The pandemic harms most people - economically, socially, mentally or else. Curbing the spread of COVID-19 can only be successful if all available resources are applied to the best of their capacities.

Lastly, we may add an argument from the perspective of fairness. One may question whether CTA technology unfairly benefits people that can afford a smartphone, or people of a certain age, cultural, social or economic group. If it were true that CTA technology only benefits its own users, it may be argued that it is unfairly beneficial in respect of certain groups of people, and indeed irrelevant in respect of collective efforts to curb COVID-19. But CTA technology does not only benefit its own users - "the benefits extend to the wider population."[24] Not only is CTA technology not unfair, its social benefits create a social incentive and responsibility for those people that can afford a smartphone to install and use the app - for their own benefit as well as for the benefit of society.

---

[24] nature.com/articles/s41598-020-79000-y

3.3. The law as a reflection of current democratic moral views

If we accept that in liberal, democratic societies, the law is a true reflection of the current moral views of the majority of the people, we must also accept the moral authority of these laws. The protection of privacy is internationally and constitutionally recognised: the United Nations' Universal Declaration of Human Rights of 1948, the European Convention on Human Rights of 1950, the European General Data Protection Regulation of 2016 ("GDPR"), and South Africa's Constitution of 1996 and Protection of Personal Information Act of 2013 ("POPIA") explicitly list the protection of privacy as a basic human right - a fundamental, natural right given to each and every autonomous, free individual.

However, all of the above authorities allow for exceptions to privacy protection, if 'reasonable justifications' can be provided. The European Convention on Human Rights states that public authorities may interfere with the exercise of the right to privacy if this interference is "... in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." The General Data Protection Regulation states it as follows: "The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality." South Africa's constitutional protection of privacy must be read in conjunction with its general 'limitation of rights' of article 36. The Protection of Personal Information Act, which gives effect to the Constitution's right to privacy, states as its purpose in its Preamble and in article 2, to safeguard and regulate that balance between the

constitutional right to privacy on the one hand, and the free flow of personal information on the other. "Recognising that (...) everyone has the right to privacy (...) [we must bear in mind that] consonant with the constitutional values of democracy and openness, the need for economic and social progress, within the framework of the information society, requires the removal of unnecessary impediments to the free flow of information, including personal information."

3.4. A reasonable compromise

In a modern ethical context that is founded on and justified by rational arguments, the reasonable way to resolve a moral dilemma is by finding a compromise between radically opposing options - an approach that is central to virtue ethics, and the approach that the South African government has seemingly opted for. A compromise - or in the words of the father of virtue ethics, Aristotle: 'golden mean' - is an action that sits comfortably in the middle between two opposing moral options and finds its justification in its reasonable respect for both.

Bluetooth technology is a compromise between the technological possibilities at our disposal today and the protection of our privacy. Of all technological options available today, Bluetooth is the least intrusive because it operates by communicating with nearby devices by means of anonymous random codes without the need for privacy intrusions. Other countries, like China, South Korea, Israel and Poland have reportedly used geo-location and facial recognition in their efforts to curb the spread of COVID-19, and have gained radically better results from CTA technology, but have done so at the radical cost of people's privacy - a cost that cannot be reasonably justified in modern liberal societies based on the individual autonomy of their citizens.

4. DECIDE

Our analysis above has identified two agents that are in a position to make an autonomous decision which, each in its own right, may pose risk to other people. The South African government decides whether the CTA should be compulsory or voluntary, and how privacy-intrusive the CTA technology is allowed to be. On the other hand, given the fact that the CTA is voluntary, South African citizens may decide whether or not to use the CTA. The government's decision may pose a risk to all South Africans, in that not making the CTA compulsory and running it on less efficient technology may slow down its efforts to curb the spread of Covid-19, while making the CTA compulsory and more efficient requires more drastic privacy intrusions. On the other hand, individual South Africans may pose a risk to the people around them and to collective efforts to curb COVID-19 by not using the app.

The government needs to weigh up two opposing moral principles: collective health versus individual privacy. Maximising the collective contributions to and efficiency of the fight against COVID-19 implies that the CTA ought to be compulsory and privacy-intrusive. On the other hand, maximising respect for people's individual autonomy and liberty implies that the CTA ought to be voluntary, at the cost of a reduced efficiency of the fight against COVID-19. As it stands, the South African government has made CTA usage voluntary, based on the least intrusive technology. In leaving it up to citizens to voluntarily and autonomously decide whether or not to use the CTA and contribute to the fight against COVID-19, government shifts the moral risk and responsibility for a potentially slower fight against COVID-19 and potential privacy violations onto those citizens that decide to use the CTA, but mitigates the risk by opting for non-privacy-intrusive technology.

At this point in time it seems difficult to conclusively decide on whether Bluetooth-based CTA technology actually works in a South African context. What is clear, however, is that in the process, little harm is done. What is also clear is that should it turn out not to work, improvements will necessitate a sacrifice of CTA users' privacy and a suspension of citizens' autonomy to either opt in or out.

The South African government has made the correct decision. In a society that fundamentally respects the individual moral autonomy and liberty of its citizens, it is right for a government to leave complex and fundamental moral decisions to its citizens, even if moral unity would produce more efficient results for society. The government's decision to find a compromise between collective action and individual autonomy by leaving CTA usage voluntary and basing it on the least privacy-intrusive technology, is the correct decision to make at this point in time, given the current need for urgency and the limited information at our disposal.

5. DEFEND

My argument in favour of the Bluetooth-based COVID-19 Alert SA app is based on a reasonable compromise that strikes a rational balance between consequentialist and deontological concerns. We have seen that consequentialism in itself does not suffice, because while it may conclusively assume that Bluetooth-based CTA technology poses no harm in respect of its users' privacy, it cannot (yet) rely on adequate empirical evidence to predict benefits in respect of collective health. We have also seen in the list of arguments for and against privacy that a rights-based deontological protection of privacy runs the risk of paralysing every collective effort in the fight against COVID-19, and may go diametrically against other fundamental rights and duties.

In times of uncertainty and urgency, moral decision making ought not to be based on isolated moral theories, but ought to attempt to provide an actionable, practicable moral framework quickly. A single focus on consequentialism fails, because while it essentially relies on harm and benefit predictions to single out the best moral action, the unavailability or lack of proven certainty of these predictions paralyse its decision making. A single focus on deontology fails, because while the blind protection of rights may ignore real consequences, and the blind protection of one right may ignore the protection of another, the indecisiveness to protect one right over another, or over harmful consequences, paralysis its decision making.

Of course, paralysis is not an option. " … the lack of direct evidence does not make it ethically less urgent to reduce the risk" (Hansson, 2018). In times of uncertainty and urgency, moral decision making therefore ought to be a rational compromise between all likely consequences and valuable rights - in our case a compromise between collective health and individual privacy.

No identifiable information is being collected by the Bluetooth-based CTA, and therefore the recurring criticisms of privacy-intrusive technology simply do not apply. While there are good reasons to distrust some of the claims made by big tech companies[25] and governments[26] I do not believe that unsubstantiated assumptions or suspicions at this point warrant a blanket refusal to contribute to an urgent and likely effective early COVID-19 detection and prevention system.

---

[25] When it comes to their users' privacy concerns, big tech companies like Facebook and Google have repeatedly demonstrated an attitude of "Move fast and break things. Big tech's strategy has been to do what they please until they face resistance. Once resistance is encountered, big tech usually tries to ignore it. When that doesn't work, they try to seduce people with extra perks, and to exhaust their critics with endless empty responses. Only when resistance is persistent does big tech take a step back, and usually after having taken many steps forward" (Véliz, 2020).

[26] For example, while the government of Singapore had repeatedly claimed that data collected via its TraceTogether programme would not be used for anything other than virus tracking, it later admitted that it made the data available to the police for the purpose of criminal investigation (bbc.com/news/world-asia-55541001).

Legally speaking, POPIA does not apply to de-identified personal information "to the extent that it cannot be re-identified again" (Section 6(1)(b) POPIA). POPIA defines de-identified information more specifically as personal information that cannot be used, manipulated or linked to other information by a *reasonably foreseeable* method to identify a person (Section 1 POPIA). Because South Africa's Bluetooth-based CTA does not collect personal information that may be "reasonably foreseeably" re-identified, the COVID-19 Alert SA app is POPIA compliant.

In conclusion, because no identifiable personal information is collected by South Africa's Bluetooth-based CTA, and because urgency in the fight against COVID-19 can not allow us to wait for conclusive data about the actual efficiency of Bluetooth-based CTA technology in a South African context, and because while current CTA usage may not yet have produced verifiable evidence of its actual behavioural and collective health benefits, no actual or potential harm can be identified either, I advise everyone that can afford it to install the COVID Alert SA app on their smartphones and contribute to the collective fight against COVID-19.

Reference list

* DeBrabander, F. (2020). *Life after Privacy, Reclaiming Democracy in a Surveillance Society.* Cambridge : Cambridge University Press (Kindle Edition)
* Cullison, A. (2018). *The Ethics of Privacy Online with Andy Cullison* in Examining Ethics podcast 24 May 2018, available at examiningethics.org [Accessed 6 March 2021]

* de Montjoye, YA., Hidalgo, C., Verleysen, M. et al. (2013). *Unique in the Crowd: The privacy bounds of human mobility*. Sci Rep 3, 1376 (2013). Available at doi.org/10.1038/srep01376 [Accessed 4 April 2021]
* DOH Department of Health of the Republic of South Africa (2020). *Covid-19 South African Online Portal*. Available at sacoronavirus.co.za/2020/09/01/download-the-app-every-covid-alert-sa-app-download-means-more-lives-saved-in-sa/ [Accessed 21 March 2021]
* Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dörner L, Parker M, Bonsall D, Fraser C. (2020). *Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing*. Available at pubmed.ncbi.nlm.nih.gov/32234805/ or at research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown. [Accessed 21 March 2021]
* Floridi, L. (2013). *The Ethics of Information*. Oxford : Oxford University Press (Kindle Edition)
* Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford : Oxford University Press (Kindle Edition)
* *General Data Protection Regulation* (GDPR) 25 May 2018, Available at eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 [Accessed 20 March 2021]
* Gilbert, S. (2021). *Good Data. An Optimist's Guide to our Digital Future.* Welbeck Publishing (Kindle Edition)
* Hansson, S.O. (2013). *Fair Exchanges of Risk*. In: The Ethics of Risk. Palgrave Macmillan, London. Available at https://doi.org/10.1057/9781137333650_7 [Accessed 22 March 2021] pp 97-110
* Hansson, S.O. (2018). *How to Perform an Ethical Risk Analysis (eRA)*. Risk Analysis. Vol. 38 No 9, 2018. DOI: 10.1111/risa.12978.

* Hayenhjelm, M. & Wolff, J. (2012). *The Moral Problem of Risk Impositions: A Survey of the Literature* in the European Journal of Philosophy. Available at philpapers.org/rec/HAYTMP [Accessed 27 March 2021]
* Hermansson, H., Hansson, S. O. (2007). *Three-Party Model Tool for Ethical Risk Analysis*. Risk Manag 9, 129–144. Available at doi.org/10.1057/palgrave.rm.8250028 [Accessed 27 March 2021]
* Jagers, S.C., Harring, N., Löfgren, Å. et al. (2020). *On the preconditions for large-scale collective action*. Ambio 49, 1282–1296. Available at doi.org/10.1007/s13280-019-01284-w [Accessed 27 March 2021]
* Olson, M. (1965). *The logic of collective action: Public goods and the theory of groups*. Cambridge: Harvard University Press
* *Protection of Personal Information Act* (POPIA) 2013, Available at justice.gov.za/inforeg/docs/InfoRegSA-POPIA-act2013-004.pdf [Accessed 20 March 2021]
* Richterich, A. (2018). *Big Data: Ethical Debates.* In The Big Data Agenda: Data Ethics and Critical Data Studies (pp. 33-52). London: University of Westminster Press. doi:10.2307/j.ctv5vddsw.5
* Sandberg, J. (2011). *My Emissions Make No Difference: Climate Change and the Argument from Inconsequentialism* in Environmental Ethics. Available at philpapers.org/rec/SANQEM [Accessed 27 March 2021]
* Seynhaeve, J.A. (2020). *Are we morally obliged to share personal information?* Available at jeroenseynhaeve.com/are-we-morally-obliged-to-share-personal-information/
* Véliz, C. (2020). *Privacy is Power. Why and How You Should Take Back Control of Your Data*. Transworld. Bantam Press. ISBN 9781787634046 (Kindle Edition)