Privacy, Technology and Public Health: an Ethical Reflection with a Particular Focus on the Covid-19 Crisis Case

John Cabot University

Department of History and Humanities

Bachelor of Arts in Humanistic Studies

Minor in Psychology

Privacy, Technology and Public Health: an Ethical Reflection with a Particular Focus on the Covid-19 Crisis Case

Francesca Dalmazzo

First Reader
Stefan Sorgner

Second Reader
Annette Bryson

Spring 2021

Abstract

This thesis will primarily investigate the ethics of developing technology as a tool for aiding public safety and public health. Since recent technological advances have become more and more pervasive, people's personal data is consequently monitored through technologies such as social media, tracking apps, and cameras. Therefore, this has given rise to worries about privacy and, in particular, worries about people's control over their personal information. In my project, I examine some ethical considerations regarding the use of technology to monitor people's private lives, in order to contain health disasters such as a pandemic. More specifically, I focus on the *Immuni* app currently being used in Italy with the aim of containing the spread of Covid-19. I explore considerations that can help us find an equilibrium between personal privacy and the good of public health. I also focus on the *obligatoriness-voluntariness* dichotomy that may arise when it comes to downloading tracking apps. In this project, I assume the consequentialist moral theory *utilitarianism*, and conduct my investigation from that perspective.

Dedication

To all those who are still here, to all those who keep fighting. Never give up.

Acknowledgements

The realization of this thesis would not have been possible without the encouragement, patience and insightful comments of some important people.

Thank you, Professor Sorgner, for your constant support and for your precious help. You have been a true source of inspiration and one of my favorite mentors. I am really grateful to have had you as my first reader.

Thank you, Professor Bryson, for your guidance and your enthusiasm, which have been two significant and unforgettable components of my last semester at JCU. I could not have asked for a better second reader.

Thank you, Manlio, for your endlessly valuable help, for guiding me through the APA style and for giving me a lot of helpful suggestions.

Thank you, Professor Antomarini, for your wonderful teachings which have contributed to make my three years at JCU so much inspiring. Since my very first semester, I have realized how passionate you are about what you teach, and I will definitely keep your lectures in my heart.

Thank you, Professor Luti, for passing down to me all your love for Psychology and for stimulating me, every day more. I feel I have learned so much from your lectures, and I will be forever grateful for that.

Thank you, S, for always being there for me, no matter what. As I told you many times, you are and will always be my daily ray of sunshine and I could not imagine how my life would be without you by my side.

Thank you, Z, for always pushing me toward my goals and for constantly supporting me, even in my darkest and craziest periods. Thank you for understanding my initial concerns and doubts about this thesis. Trust me when I tell you that you truly deserve the world.

Thank you, O, for always comforting me and for always giving me the strength to push forward.

Thank you, mum, dad, and Fede, for always believing in me, for giving me your support even if we live far away from one another. All this would have not been possible without you.

Table of Contents

1. Introduction

2020 will be always remembered as the year in which the spread of SARS-CoV-2 (Covid-19) changed the life of the entire global population. Within a few months of the very first (known) cases of Covid-19 appearing in China (in November 2019), medical professionals and other experts from all over the world came to understand just how dangerously pervasive the virus was. Although early on the impact of Covid-19 appeared to be somewhat like that of a bad flu, the exponential growth of ascertained deaths and infections soon revealed that the virus was actually much more alarming. For this reason, on 11 March 2020, the World Health Organization (WHO) officially declared Covid-19 to be a global pandemic (Klar et al., 2020). From that moment on, most countries began implementing a wide variety of measures designed to contain the spread of the virus.

Italy is among those countries which experienced an extremely high number of lives loss from Covid-19 starting from the first wave of contagion (i.e., in March 2020). For a nation that counts approximately 60 million inhabitants, the death of about 100 thousand people (together with the infection of nearly 2 million people) is an incredibly serious issue, one that from the beginning has required large-scale solutions aimed at protecting the safety of everyone. In response to the urgency of the situation, the Italian government took the drastic decision of enacting an obligatory and unprecedented national lockdown (which began in March 2020). This lockdown resulted in the total closure of every type of commercial activity (from bars and restaurants to shops) as well as the closure of schools and universities. Only supermarkets, pharmacies, and some other

businesses that provide basic necessities were allowed to stay open. Even hospitals, which, of course, remained opened, cancelled most non-urgent appointments. All people who could work from home (in smart-working mode), including students, were allowed to leave their places of residence only for very specific reasons, such as going out to buy food or medicine, and they were required to carry a pass with them on such occasions. Furthermore, when outside of their homes, everyone was required to wear a facemask and to maintain a 1-meter social distance from any other people.

Not surprisingly, these quickly enacted and unexpected restrictions brought about stark disagreements. These types of restrictions were put in place with the goal of protecting the Italian citizens from a public health and medical point of view. Nonetheless the impact on the lives of many people in Italy was devastating from an economic and psychological point of view. For many people, staying at home was tantamount to losing their jobs; indeed, during the year 2020, nearly 450 thousand Italian people lost their jobs and the Italian GDP (Gross Domestic Product) decreased by 8%. (Amato, 2021) Additionally, the social isolation that was an inevitable part of the lockdown for so many people led to increased loneliness and sadness. People found themselves in a state of "permanent uncertainty and [were faced with] dramatic changes to personal plans, not to mention realistic fears of being infected" (Wnuk et al., 2020, page 2). In brief, several areas of people's everyday routine suddenly and dramatically changed; plus, what scared everyone the most was that no one initially knew for how long all these restrictive measures would last. Consequently, in an attempt to limit all these negative outcomes, the Italian government (together with the Ministry of Public Health and the Minister for Technological Innovation and Digitisation)

decided to rely upon technology, releasing a mobile app called *Immuni* which represents a form of digital contact tracing aimed at containing the spread of the virus.

Basically, when you download this app (which is free), you are given a casual numeric code, that changes every fifteen minutes. The app *does not* require personal information and data (meaning that it does not require names, surnames, private addresses and so on) but rather asks you to keep the Bluetooth signal on at all times in order to register the codes of those with whom you have been in contact. In brief, "the methodology required is a continual loop of testing and identification of those infected, finding those who have been in contact with COVID-positive individuals and quarantining and testing them" (Hart et al., 2020, page 5). Although the main purpose of the app is that of minimizing the spread of Covid-19, it also "seeks to limit the amount of data collected and used to the minimum necessary" (Rothstein, 2020, page 1374). This idea can be related to the "data minimization" concept (Rothstein, 2020), according to which personal data should be safely collected and stored just for specific purposes and for a limited amount of time. Importantly, however, in order for the *Immuni* app to be really effective, and therefore to bring about the clear social good for which it was intended, on average, 65% of the Italian population would need to use the app.

Of course, digital contact tracing opens up a series of philosophical questions. For example, some concerns are related to the ethical aspect of incessantly monitoring and checking people's movements and contacts by means of technology. Further, there are questions we must ask focused on issues such as inequality: it is very likely that not every single person possesses a smartphone from which to download tracking apps. Finally, but perhaps most importantly, the use of such

tracking apps give rise to questions about the likely implications of tools of mass surveillance or about the fact that personal data could be possibly exploited by the government, even in the future.

In spite of a wide range of concerns about such apps, it is also very important to take into consideration the fact that digital contact tracing represents an ideal solution if our goal is to avoid generalized lockdowns and mass quarantines, with all of their accompanying and potentially devastating consequences to the lives of people (see above). In turn, avoiding generalized lockdowns appears to be the first step toward economic recovery. In addition to all of this, digital, as compared to more traditional, hands-on, contact tracing frees up medical personnel, who, in turn, can focus more on patient care, which, in this alarming situation, is an urgent need. Compared to traditional contact tracing, then, this system actually represents a much faster and safer type of approach to measure and control Covid-19 infections. Finally, digital contact tracing is more trustworthy than more traditional hands-on contract tracing because it completely relies on algorithms and not on human memory. In brief, through the use of tracking apps, we could be able to slow the spread of the virus, while "saving millions of lives, preserving social stability" (Hart et al., 2020, page 5) and avoiding additional economic crises.

My thesis focuses on the question: "Should the use of the *Immuni* app be made legally obligatory to trace people's contacts in order to prevent the spread of Covid-19?" In order to elaborate my own answer, I will first consider both the pros and cons of tracking apps with a particular focus on the *Immuni* app. I will then argue that, despite clear problems with doing so, on balance, the ethical considerations count in favor of making the use of the Italian *Immuni* app legally obligatory. I will defend this primarily from a consequentialist, and in particular broadly utilitarian, perspective, and argue that the current state in Italy (at the time of writing) is one of

“exception”, namely, one in which the benefits to public health and safety that we can expect to be the result of the use of digital tracking apps outweigh the potential harms to individual rights, such as the right to privacy, that can result from them. Concerning the structure of my project, I will first introduce a small debate regarding both the positive and the negative aspects of making use of technology on a daily basis. I will then focus my analysis on tracking apps, by highlighting their main characteristics and strongly arguing in favor of their usage to contain the spread of Covid-19. Further, I will take into account some of the main arguments against my position, including privacy concerns and the inequality factor. I will also introduce an explanation of what I mean by “state of exception” by drawing parallels with other historical cases in which the adoption of some exceptional means was justified by the “newness” and the “riskiness” of the context. Finally, I will justify my own position by relating to the philosophical theory of utilitarianism.

2. Literature Review

As of the beginning of 2021, the spread of Covid-19 virus has posed a series of challenges, not only from a medical point of view, but also from an ethical or moral one. One such challenge stems from the development of various tracking apps and surveillance technologies by a number of governments in an attempt to help prevent the spread of the virus. Within this context, a growing number of researchers have been exploring the ethical implications of using these various technologies designed to combat or slow the spread of Covid-19. Of particular interest for my purposes are the implications for privacy, indeed, the tension that often arises between providing privacy and the potential benefits gained by all from the use of technology. In what follows, I will be taking into account some of the sources on which I will be focusing in this project. I will highlight their main strengths and weaknesses, showing how they may be related to one another and how they may fit into my thesis.

Goodman (2020) and Klar et al. (2020) both argue that, although posing challenges of effectiveness and risks to privacy and equity, Covid-19 tracking apps represent a promising solution to fight against the virus, in particular if we want to avoid mass quarantines and lockdowns. The general working principle of tracking apps is quite simple: the Bluetooth device associated with your smartphone records all the contacts you have had and in case one of them has resulted positive it warns you to take precautions. The question around which the two authors formulate their reflection is essentially "what is the right balance between protecting individual privacy and reducing the virus' spread?". Goodman (2020) analyses the issue by relying on a utilitarian framework; further, both Goodman and Klar et al. (2020) focus on the "ethical design"

of tracking apps. According to Goodman (2020), what matters the most in this complex and unprecedent situation is people's wellbeing, and, he argues, the benefits to people's wellbeing from the use of tracking apps is so great that it clearly outweighs "the potential harms to individual rights" (page 1). It follows, therefore, according to his view, that the right thing to do is to make use of digital contact tracing methods. The approach elaborated by Klar et al. (2020) is more nuanced. Their focus is more on the elaboration of a set of questions a tracking app should positively answer in order for it to be ethically acceptable and, therefore, appropriately respectful of people's privacy. Although Goodman (2020) only gives a short definition of utilitarianism without mentioning possible pros and cons, both articles are relevant for my study because they provide valuable and multilateral views and explanations of the concept of privacy in relation to technology.

In a similar way, Akhlaghi (2020) engages in a reflection on how our freedom may be threatened by the various anti- Covid-19 measures imposed by most governments all around the world. Although Akhlaghi (2020) does not address the issue of tracking apps in particular, focusing instead on the obligation to wear facemasks, his argument can be expanded in order to apply it to the issue of tracking apps. Olson (2020) too does not directly address the issue of tracking apps, but the sorts of issues he addresses give rise to some of the same ethical questions associated with tracking apps. In fact, Olson (2020) describes how a number of offices in the United States have been re-arranged to meet the government guidelines regarding social distancing. The transformation includes the installation of tiny cameras that, through infrared technology, use "computer vision […] to count how many people are in a room and measure how far apart they are" (Olson, 2020, page 1). Although this kind of technology does not record faces but only moving

bodies, people are tracked. So, is the freedom of workers somehow compromised? Are people's rights violated in some way? To answer such questions, we can focus on the distinction highlighted by Akhlaghi (2020) between *infringement* and *violation* of a right. According to Akhlaghi (2020), in the case of the current Covid-19 pandemic, the measures that have been adopted do not represent violations of rights but rather merely infringements of rights, because "we act wrongly in imposing significant risk upon others if we refuse to follow these measures" (Akhlaghi, 2020, page 2). This reinforces and expands upon Goodman's idea (2020) according to which we are justified in violating the privacy and the freedom of a few people in order to assure the welfare of many people. I agree with these various authors that in the context of the current global pandemic, there is compelling reason for privacy rights to be moved to the background and for primary focus to be on public health and safety.

Even if we accept that in the context of a global pandemic the benefits to public health count decisively in favor of using tracking apps, in spite of privacy concerns, the question remains whether the use of such apps should be voluntary. Klar et al. (2020) claim that the use of technology has to remain voluntary in the sense that people, for privacy reasons, should not be forced in any way to download tracking apps. Even the mere decision to carry a smartphone (which represents the first step toward digital contact tracing) should be voluntary. Furthermore, the authors maintain that people who decide not to use or who uninstall the app should not be punished in any way. Precisely what counts as voluntariness of use, however? Klar et al. (2020) draw an important distinction between genuine and only apparent voluntariness. They mention the example of China, where people are obliged to use tracking apps if they want to enter specific public areas. It turns out, the authors maintain, that though the use of tracking apps is voluntary, the strict

restrictions imposed by the government "make it de facto compulsory" (Klar et al., 2020, page 5). In brief, people are denied a certain degree of freedom, and Klar et al. rightfully maintain that this is problematic. In some contexts even though the use of tracking apps is technically completely voluntary, both Klar et al. (2020) and Stoops (2020) explain that people have good reason to be reluctant to use such apps because they have reason to be uncertain about where data will go, who will have access to the data and for how long they will be kept. Other authors highlight such worries even in the context of countries where use really is voluntary. Wnuk et al. (2020), for instance, highlight worries about the fact that private data could be used for other purposes (including commercial ones). Wnuk et al. (2020) emphasize, however, that in spite of such worries, which must be taken seriously, this current situation is a perfect example of the so-called "state of exception". This means that the current situation is one in which exceptional actions need to be taken so that the existing and "normal" order can be preserved and in order to guarantee the safety of citizens. In such contexts, as the authors maintain and as I will argue, the violation of certain rights can be justified. Wnuk et al. (2020) further argue that people tend to recognize the importance of this tradeoff, pointing out that, under threat, people are generally more willing to accept restrictions on their freedom in order to enjoy more of a sense of security. At the same time, the more the need for security is salient to people, the less they tend to be concerned about privacy. In short, though all of these authors recognize the importance of rights such as those associated with freedom and privacy, they maintain that they are surpassed in importance by the need to preserve people's health and safety. Although articulating their arguments in different ways, all these sources constitute possible answers to one of my research questions, which is "How challenging is it to balance public safety and personal privacy in the digital age?".

As mentioned earlier, one additional ethical challenge that tracking apps pose is the question of "inequality". As a matter of fact, it is not the case that every single person on this planet can take advantage of this type of technology. Many people, for instance, cannot afford to have smartphones, and thus cannot afford to have access to track apps. Furthermore, many older people or children may not have access to such devices. We can easily predict, therefore, that the pros and cons of tracking apps use are unlikely to be distributed equally amongst the population. This is an issue highlighted by Klar et al. (2020). In a similar way, Stoops (2020) argues that Covid-19 has hit, in particular, poor areas in which low-quality health care and the lack of hygiene have worsened the situation. In such contexts, it may be very difficult for people to access tracking apps, mainly because they first have to deal with more urgent problems. Although most of the literature on the topic promote the use of tracking apps, only a few articles reflect on the "inequality" component, which is a fundamental one. Authors such as Goodman (2020), for instance, mentions how important it is to further develop contract tracing but considers privacy the only obstacle that may arise, not taking into account additional factors.

Thus far, I have focused primarily on people's hesitant attitudes towards the new measures elaborated by the government. But what if people are willing to download tracking apps? What would motivate them? Wnuk et al. (2020) identify two main factors, that are actually related to another: a lacking sense of personal control and, of course, the perceived threat of Covid-19. Firstly, Wnuk et al. (2020) argue that, being the Covid-19 pandemic difficult to personally control and counteract, people may feel trapped in a generalized "sense of uncontrollability"; therefore, in this type of situation, the *compensatory control model* makes people very likely to re-establish their sense of certainty by relying on those in power. In other words, people's acceptance of new

forms of surveillance technology may represent an example of an indirect tool for regaining a sense of control. Secondly, people are very likely to feel threatened by the Covid-19 virus both for themselves and for their loved ones. Consequently, Wnuk et al. (2020) hypothesise that "the level of personal threat related to the Covid-19 pandemic would inspire greater support for the implementation of anti-epidemic technologies that involve a trade-off between civil rights and security" (page 4). Goodman (2020) adds that people are motivated by the fact that, as long as they prove to be effective, easy to use, and careful about one's privacy, tracking apps and surveillance technologies could allow millions of people to return to work and millions of children to go back to school. In other words, hoping that their contribution will be somehow helpful and that they will be able to see long-term positive results, some people could be more willing than others in downloading tracking apps.

3. The Role Played by Technology

In a world dominated by electronic devices, apps, social media, and numerous other advanced forms of communication, society's reliance on technological means is increasing more and more. Often conceived to be just a tool, technology actually has broader implications. Indeed, technology shapes both the space we inhabit and our conception of sociability (Sandler, 2013). As a matter of fact, if we want to see a friend or pay our bills, our physical presence is no longer needed: we can easily meet our friend online and we can avoid the line at the post office by taking advantage of the various websites that allow us to make online payments. Furthermore, advanced technology is becoming more and more important in the area of health care, as it plays a fundamental role with respect to the treatment of serious medical issues. Technology plays a significant role in helping improve the lives of people with disabilities too; think, for example, of blind children who can now see YouTube videos through the *Video4Blind* system, or learn numbers and words through an audio-app (called *Math Melodies*) elaborated by the University of Milan (Naccarato, 2015). In other words, technology has come to facilitate our lives and wellbeing in ways that may not have been easily conceivable even a few years ago. One striking example of this is the capacity for technology to play a significant positive role in situations such as a global pandemic. As of 2021, in response to the Covid-19 pandemic, a number of national governments have created and relied upon tracking apps, which help identify potential exposure at a rate many times faster and more efficient than more traditional "on-foot contact tracing" methods.

In spite of the clear advantages to much of the technologies that are now a significant part of people's lives in many societies, there are clear risks. Perhaps most strikingly is the fact that the pervasiveness of technology in many societies makes it far easier for people in power to "engage not only in mass surveillance, but also to process data from that surveillance in a way that no human actor previously could" (Davisson et Booth, 2016, page 3). In light of this, it is important for us to consider a number of potential moral implications. One real worry is that if we are constantly observed and monitored through digital systems, we may be deprived of our right to freedom and privacy. On the other hand, the advantages to our health and overall wellbeing of the use of some of these surveillance technologies are clear. It is important, therefore, that we are cautious and that we carefully weigh the pros and cons of the use of various technologies in specific contexts. We must ask whether there are contexts in which our privacy takes second place to some other consideration, and, if so, specifically under what conditions.

In this thesis, I focus particularly on the so-called *information* technologies, a term that "refers to automated systems for storing, processing, and distributing information" (den Hoven et al., 2010, page 59). More specifically, what are some examples of information technologies? We can definitely say that social media, tracking apps, mobile devices, and the Internet in general are part of this category. Nissenbaum (2010) argues that all these different examples of technologies can become dangerous whenever they enable "pervasive surveillance, massive databases, and lightning-speed distribution of information around the globe" (page 4). As a matter of fact, all these various types of technology allow us to get everyday news and information of all kind. Consequently, in order to make people's lives simpler, information technologies collect a great variety of data, including health and fitness data, social media content, and location and movement

data (Vitak et Zimmer, 2020). These sorts of technologies have been seamlessly integrated into many people's lives. However, while people may feel comfortable with using something like Google Maps to get driving directions, many people seem to be far more cautious about and even resistant to the idea of entrusting the government with the management of their personal information, such as in the case of tracking apps. Although these two examples may sound far from one another, they are actually more similar than people seem to realize: in both cases we are relying on technological means in order to solve or ameliorate everyday issues (first case) or the spread of a threatening virus (second case).

The massive use of information technologies (and, in particular, of *Internet-based* technologies) brings about a quite important concept, which is that of mass surveillance or, in this specific case, the so-called *Internet Panopticon*. The term *Panopticon* was originally used by Jeremy Bentham (in the late 18th century) to refer to a kind of structure, in Bentham's case a prison facility, in which, thanks to a particular architectural structure, prisoners could be constantly observed by the guards. The prisoners could not see the guards, however, so they could never be certain when they were or were not being observed. In today's society, a far broader range of people can be observed and perhaps even controlled in large part thanks to the Internet, hence the term *Internet Panopticon*. Note, however, that whereas with Bentham's *Panopticon*, it was clear who was the guard and who was the prisoner, so who was being observed and who was doing the observing, with respect to the *Internet Panopticon*, "any person who is living in a technologically advanced society is (at least in principle) part of it" (Sorgner, 2021, page 72). Furthermore, "the situation is even more complex because the individual roles of guards and prisoners are less clearly defined" (Sorgner, 2021, page 73). Given that the *Internet Panopticon* is a virtual space, things get

even more complicated. This situation gives rise to a number of important questions including, most notably: Who is watching us? Who is in charge of keeping our data? What is striking is that the answers to these questions are almost never clear: on the Internet today we can find every kind of information very easily and, given the speed of technology's evolution, it is very likely that our data will be more and more accessible to our "virtual" public. However, while on the one hand a mass surveillance type of system is not very likely to be accepted by the vast majority of the population, on the other hand I argue that a global pandemic, such as the Covid-19 pandemic current at the time of writing, counts as what can be called a "state of exception"; this term refers to a situation in which "the violation of certain laws is justified to preserve the existing order" (Wnuk et al., 2020, page 2). In particular, I argue that we have good reasons to embrace the use of tracking apps as a method for combatting the pain and suffering as well as the loss of lives during a global pandemic, and specifically during Covid-19 pandemic of 2020 (and which is still active during the time of writing).

However, there are legitimate reasons to be cautious about the use of tracking apps. For example, people may be worried about a privacy violation, which would possibly result in an exploitation of their data by the government, not only in this particular situation, but also in a distant future. Not all tracking apps pose the same risk, though. Indeed, it is important to underline a fundamental distinction between tracking apps that are more and those that are less easily to de-anonymise, meaning subjected to personal information's disclosure. For instance, though there are pros and cons to each type of tracking app, Bluetooth-based apps (like the *Immuni* app) are more difficult to de-anonymise than those based on GPS or WiFi systems. In fact, while GPS-based apps are more concerned with tracking users' physical *locations*, Bluetooth-based apps record users'

physical *contacts*. So, while on the one hand GPS tracking is useful because it cautions people to avoid areas that may be at high risk of infection, on the other hand "it is less accurate at identifying whether two people have been at the same place at the same time" (Hart et al., 2020, page 21). But Bluetooth-based apps are not flawless either. As a matter of fact, they are more accurate in terms of recording both duration and proximity of in-person contacts because they work efficiently in most contexts, including underground and indoors environments (Hart et al., 2020). They are also rather reliable in terms of information storage because, generally, data can only be seen on and by the users' phone (and not sent to third parties). However, as Abbas et Michael (2020) point out "proximity and duration information can reveal a great deal about a user's relative distance, time and duration of contact. A Bluetooth-based app may not know where you are on Earth's surface, but it can accurately infer your location when bringing a variety of data together" (page 1). As seen, that of tracking apps is a very complex and multidimensional issue because of its several implications, including security risks and government abuse. Therefore, it is hard to find a technical solution which guarantees absolute privacy.

It is important to note that even traditional (or manual) contact-tracing, although less invasive as an approach, does not fully protect individuals' privacy either. It is not clear, therefore, that it is worth giving up the far greater benefit to society from the use of tracking apps as compared to more traditional contact-tracing. Basically, traditional contact tracing first involves the isolation of the person who has tested positive for the virus; then, this person is usually asked by medical personnel to list all the contact he or she has had, in order to isolate as many people as possible in a relatively short period of time. As seen, this approach already implies the disclosure of personal information to third parties and "makes a trade-off between the privacy of a positively tested

individual and the benefits to society" (Chan et al., 2020, page 2). More traditional methods have been shown to work well when there is a rather limited number of infected people, such as during the outbreaks of Ebola and HIV at the beginning of the 21st century (Hart et al., 2020). They are clearly far less effective, however, when the numbers of people infected are as high as they have been during the Covid-19 pandemic.

There are some additional downsides to traditional contract-tracing methods that need to be underlined. The first one is related to the fact that traditional contact tracing depends upon human memory and, for this reason, may not be very reliable. In fact, it may be hard for people to recall all contacts they have had. This, of course, increases the chances of more potentially sick individuals going around and infecting even more people. Another crucial aspect that ought to be considered is time; traditional contact tracing takes a good deal more time than tracking apps, and, in such an alarming situation as the Covid-19 pandemic, speeding up the entire process of recovery must be a fundamental priority. Indeed, numerous lives can potentially be saved by speeding up contact-tracing processes. One final note: one reason that traditional contact tracing takes more time is because it requires the presence of trained medical personnel, whose tasks are those of manually registering contacts and doing follow-up. However, given the extremely high number of Covid-19 victims, medical human resources are needed primarily in severely urgent contexts, such as in intensive therapies. Relying on manual contact tracing would mean hiring and training additional people and, again, there is not so much time available currently.

Consequently, following what I have just stated, I argue that digital contact tracing represents the ideal and most suitable solution (at least during the current Covid-19 pandemic) for the following reasons. First, it constitutes a more accurate and precise way to track individuals'

contacts because it relies on tokens and codes that are generated and sent to users automatically. Therefore, individuals are not asked to remember and report the names of all the people they had been in contact with because the entire process is automatic, with tokens sending and receiving alerts in case of actual infection; also, this quickly prevents people from infecting others and results in prompt self-isolation. Concerning time, then, digital contact tracing is meant to shorten the risk of exposure and to enable "health-care providers to suppress the virus rapidly" (Hart et al., 2020, page 11). Moreover, thanks to all this automatization, we would not need trained interviewers and medical human resources to spend their time focused on tracking. Finally, given the greater efficiencies outlined above, tracking apps can help societies avoid generalized lockdowns and mass quarantines. By testing and isolating only those who have tested positive, all those who are not sick with Covid-19 can go back to work, keep their commercial activities open and contribute to fasten up the economic recovery. As demonstrated, the use of tracking apps has several advantages compared to traditional contact tracing, not only from a medical and health-related point of view, but also from an economic one. Therefore, why should we not take advantage of digital tracking apps that help us accelerate the process of identification of Covid-19 positive individuals through automatic algorithms while, at the same time, saving medical workforce?

Though there are legitimate concerns about tracking apps, I maintain that when we carefully weigh the costs and benefits associated with their use, the best conclusion to draw is one in favor of their use. It is important to address concerns about the use of tracking apps, however. I have already mentioned some of these concerns above. Here I mention what I take to be a less serious concern before returning to arguably the most serious concern, namely, the worry that even if we grant that tracking apps will lead to the best consequences in the context of the current Covid-

19 pandemic, there is the possibility that, especially over the long term, their use could result in clearly undesirable consequences.

First, the less serious worry. Some people are concerned about the fact that people could deceitfully report their positivity for Covid-19 in order to spread panic or to prevent people from going out "in order to shut down school or even to disrupt an election" (Cranor, 2020, page 24). I maintain, however, that these occurrences are very rare because, before sending out the notification alert, health authorities strictly verify one's positivity to Covid-19 and, therefore, false positives are hard to find. In fact, as soon as one gets the notification about a recent contact with a positively-tested individual, this person is obliged to quickly get a swab done and then, if this person results to be positive to Covid-19, he/she has to quickly report it to the app, which, in turn, sends out the notification alert automatically.

As mentioned above, the most significant concern about tracking apps has to do with worries about privacy violations, and, in particular, the possible exploitation of people's data by the government, not only in this particular situation, but also in a distant future. This is related to worries about the so-called "function creep", according to which data collected by technological devices for good purposes are later used for different, and often questionable, ends. This means that, since people's data (although minimal) constantly circulate from our devices to third parties (Vitak et Zimmer, 2020), national governments could exploit them to monitor people's health status, movements and ways of living, even in the future. Further, if we consider that, most of the time, we know little (or even nothing) about where our data will go and who will have access to them, it becomes clear that this issue is even more complicated than it might see at first.

In this context, an important concept which I will be discussing is *contextual integrity*, a theory elaborated by Nissenbaum (2004). According to this idea, the dichotomy *private vs personal* is relative and cannot be applied universally to every single type of situation. Further, contextual integrity states that "our interactions- with other people, institutions and technologies- occur in particular contexts and norms of appropriateness govern people's expectations of how personal information should flow within a given context" (Vitak et Zimmer, 2020, page 2). Nissenbaum talks about four main parameters that one should follow in order to evaluate norms of data flow and appropriateness: context, actor, attributes and transmission principles (Vitak et Zimmer, 2020). The first one is related to the frame of reference in which an interaction may occur; for example, the conversation between a patient and a doctor occurs in a *healthcare* kind of context. The term *actor*, then, refers to the people involved in a specific interaction. By the term *attributes* Nissenbaum means the various kinds of information that get exchanged during a given interaction. Finally, *transmission principles* "shape or constrain the flow of information" (Vitak et Zimmer, 2020, page 2). But how is this related to Covid-19 tracking apps? Well, first of all, let's take into account the context factor, which, in this particular case, refers to the medical situation of the user and has, as actors, the user itself and its local health authorities. Therefore, if the data collected by tracking apps are spread beyond these two main actors, contextual integrity may be violated and, as a result, also our privacy. However, most tracking apps (including *Immuni*) have been developed following appropriate norms of information flow. For example, the number of actors who have access to users' personal information is limited, exactly because these apps do not rely on a centralized type of authority. Further, concerning attributes, the only type of information that

circulate is about users' contacts and nothing more. Nevertheless, there is still much concern about the possibility of having our data disclosed and, consequently, of a serious privacy violation.

4. First Ethical Challenge: Privacy

The strongest counterargument to my position that we have compelling reason to embrace the use of tracking apps in order to combat a global pandemic has to do with concerns about privacy, In this section, I introduce the main ideas, beliefs and theories revolving around the notion of privacy in relation to technology.

Defined as "the state of being free from public attention or unsanctioned intrusion" (Free Dictionary), the multidimensional concept of privacy has, over the past few centuries, captured the attention of various scholars and philosophers. In the United States, the late nineteenth century saw the advent of several socio-economic and technological innovations which began to threaten "a right to privacy," a right that arguably "had been a factual reality" that people had not thought of as needing "legal protection" (Scoglio, 1998, page 53). More specifically, the introduction of the newspaper printing press and the development of photography prompted a further and broader reflection upon the notion of privacy. For example, in 1890, Samuel D. Warren and Louis Brandeis published the first key reflection on privacy in the *Harvard Law Review*, mostly to complain about what they characterized as "invasive" publications produced by journalists and reporters in their day. Warren and Brandeis stated that "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life" (Warren & Brandeis, 1890, page 195).

As Warren and Brandeis saw it, the development of more and more sophisticated technological instruments was becoming increasingly intrusive, leading to unacceptable limits to people's privacy. Here, we have an early connection being made between privacy and technology.

Warren and Brandeis urged both the importance and the need of establishing a legally approved "right to privacy". According to them, this fundamental right should be based on "a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds" (Warren & Brandeis, 1890, page 196). As we have seen, then, Warren and Brandeis were among the first to warn against what many have understood to be the perilous threat to privacy represented by technology. Arguably, it was because of their framing of the issue that "the debate about privacy has been fuelled by claims regarding the right of individuals to determine the extent to which others have access to them and claims regarding the right of society to know about individuals" (den Hoven et al., 2020, page 61).

Today, there is a wide array of approaches to the issue of technology and privacy. Daniel Solove, following the path of Warren and Brandeis, focuses his research on the possible privacy harms that may arise from the use of the new twenty-first century technologies. In response to what he takes to be serious harms, Solove created *TeachPrivacy* (early twentieth first century), an online company which provides data security and privacy trainings. Solove's work can be considered an example of the so-called *non-reductionist* conception of the value of privacy. According to this way of reasoning, "privacy is" understood to be "valuable in itself" rather than depending for its value on other moral values such as "autonomy, intimacy, democracy […]" (den Hoven et al., 2020, page 3).

In contrast to the *non-reductionist* approach is the so-called *reductionist* approach, according to which even though privacy is valuable, it is not as important as other more fundamental rights, such as the right to liberty and the right to property (Hoven et al., 2020, page

3). Some people today even defend a more extreme approach to privacy according to which privacy is not morally relevant at all. Zimmer, for instance, (as cited by Richterich, 2018) claims that privacy should not be considered worth of ethical investigation because, on platforms like Twitter or Facebook, "the data is already public" (page 77), that is to say easily accessible by the various companies' owners. It should be clear from this very brief overview that the discussion regarding technology and privacy is far from a straightforward issue. Indeed, its multilateral character and multiple dimensions make it worth of constant study and investigation.

In order to get clear about this issue, we might want to ask the following questions: What are some specific moral reasons why people are so concerned (and somehow obsessed) about their privacy's respect? Why is privacy such a valuable component of our everyday life? Ethically speaking, why is the privacy issue so relevant and significant?

First of all, privacy is related to our most private and intimate sphere, meaning that it gives us a sense of independence by representing a sort of "safe place" where we can "hide" our personal information and secrets. In this regard, Solove (2014) elaborates a series of reasons why privacy matters so much and, therefore, should never be violated. Solove claims, for example, that privacy is an issue of respect, and, if a person wishes to maintain something out of public knowledge, his desire needs to be respected. As I argue above, however, it is important to note that there may be some exceptions to this principle, and one such exception that I defend is the use of tracking apps. In light of the clear benefits in the context of this unprecedent Covid-19 situation, collecting information about users' locations and contacts should not be seen as a moral violation, but instead as a general attempt aimed at ameliorating and solving the entire pandemic.

Another important aspect that Solove (2014) emphasizes is the idea that privacy allows us to have control over our own lives, without having to constantly justify our actions or movements to someone. Privacy, Solove maintains, is a synonym for autonomy and freedom—both freedom of speech and of thought. Also, privacy can be said to enable people to control and manage their reputations, meaning that, through privacy, they share with others only what they want to share. This is related to the *prevention of harm* principle in support of the right of privacy. For example, if someone could have access to our Facebook profile or to our bank account, our personal data could be exploited in endless ways and for infinite scopes, some of which would be bad. Here again, however, though I agree that privacy is important, and though I agree that when people have access to more information, there is an increased risk that our information will be used in ways that can be harmful to us, there are nonetheless contexts in which we benefit from giving up some of our right to privacy. It is important to recognize that sometimes the prevention of greater harm requires opening ourselves up to the potential for some other kinds of harm.

It is also important to note that one further (though related) reason that privacy is highly valued is because of the fear of sanctions associated with it. Indeed, one reason we value our privacy is so that we do not have to pay the consequences for some of our actions. The more privacy is protected, the higher the chances that people can keep, for instance, their illegal actions (such as drug trafficking) or their immoral actions (such as cheating on one's partner) hidden. This idea falls into the *theory of sanctions for privacy* (Sorgner, 2021), according to which the more we maintain our data private, the fewer sanctions we fear. Taking account of this does not amount to dismissing the importance of privacy. It does help make clearer, however, that our often vigorous defense of our privacy is not always based on a desire to improve the general wellbeing.

Furthermore, a rigorous protection of privacy no matter what does not necessarily lead to the best overall consequences.

Whatever the actual consequences of other people having access to our private information, in order to make sense of privacy issues related to information technology, such as tracking apps, it is important to understand that much of the personal data of concern in discussions of privacy is already broadly dispersed. Davies (1997) points out that our personal rights to privacy have been transformed into "consumer issues" (page 150). More specifically, in a world that constantly evolves and in which national trade exchanges have been transformed into global markets, "many traditional rights have been put on a commercial footing" (Davies, 1997, page 152): Zuboff calls it *surveillance capitalism* (Goodman, 2020), that is to say a kind of market where our personal information represents the main commodity or product of exchange; essentially, this means that our data are increasingly circulating and, often, we do not even know where they will end up. Here again my point is not to say that it does not matter that our personal data is widely dispersed or that we do not even know who has access to it. The reality of this is relevant, however, when we weigh the costs and benefits of using technology to combat a global pandemic. If the primary cost of or downside to using tracking apps is that it could result in our personal data to circulate from our devices to third parties and to be used in a variety of unintended ways, it certainly seems relevant to take into consideration the fact that our personal data is already widely dispersed.

Finally, another important consideration is Sorgner's point that we highly value our privacy because it is strictly related to information and data about ourselves, which represent what we can characterize as our *property* (Sorgner, 2021). Basically, this means that what I do, who I see and

where I go are all examples of personal kind of information that I am not necessarily obliged to share with anyone. More specifically, we talk about *intellectual property* which, in this particular case, becomes a *digital* kind of intellectual property since our data constantly flows within the Internet domain. In brief, according to Sorgner's *theory of property*, "data is our intellectual property and therefore an extension of ourselves. If governments (or anybody else) take away our data, they seem to expropriate us" (Sorgner, 2021, page 99) and, at the same time, to undermine some of our fundamental rights.

Whereas I do think that we have to be careful to respect people's rights to their own property, including their intellectual property, used broadly to include information about themselves and their movements, I maintain that the type of surveillance that may derive from the use of tracking apps should not be seen as an "expropriation" of personal data. Rather, as Sorgner (2021) argues, it is best viewed as "our payment for something the majority of people regard as an important determinant of the quality of life, namely our health" (Sorgner, 2021, page 101). As I have emphasized through this paper, the use of tracking apps brings about many positive outcomes which play a role in ameliorating the entire population's wellbeing, not only from a health-related point of view, but also from a social and psychological one. In the context of a global pandemic, it is important to acknowledge that prioritizing people's health and safety is of fundamental importance, and, indeed, that people's health and safety are more important components of their overall wellbeing than are their rights to property or privacy.

It does not follow from any of this, however, that there are not important questions to ask specifically about tracking apps in order to minimize any negative impact that can result from their use. How, specifically, can we transfer this reflection on privacy into the specific and practical

realm of tracking apps? Some scholars (including Klar et al., 2020) have elaborated a series of questions tracking apps should respond positively to in order to consider their usage "morally" acceptable. Of note are the following questions: Is personal data kept as private as possible?, or, is the data used only for the intended purpose, for instance, to stop the spread of the virus?. If the app meets positively these parameters, then we have a first step towards the development of an "ethical" kind of app. More precisely, what is an ethical app? One that does not invade people's privacy but rather one that is instead concerned with the maintenance of people's wellbeing as well as their privacy. To be clear, as I argue above, even if it turns out that people's private data ends up being more widely dispersed in less than ideal ways, it does not follow that we have decisive reason not to use these apps. We do have reason, however, to make these apps as reliable as possible, however. In this regard, what matters the most is the *design* of technologies; one example of that is represented by the "privacy engineering" approach, whose main goal is that of elaborating a series of specific guidelines that technologies should follow and respect in order to be careful about their users' privacy. In order for tracking apps to be considered "ethical", what we need to remember is that data observance and protection should be the core point when it comes to developing them. And here I can firmly argue that most Bluetooth-based apps (like *Immuni*) have been designed in a way that limits third parties' access to personal data. Such apps are based on anonymous and changing tokens that are secure from a cryptographic point of view. Therefore, we can conclude by saying that, although we cannot exclude the possibility of data deanonymization, the *Immuni* app represents a safe and useful approach in the fight against the spread of Covid-19 during the current pandemic (current at the time of writing).

5. Second Ethical Challenge: The Inequality Factor

Another significant ethical challenge to the view I defend, namely, that we have compelling reason to use tracking apps to combat Covid-19, can be characterized as the inequality factor. This has to do with the fact that, unfortunately, there is a large portion of the population who cannot make direct use of tracking apps and thus the concern is that the use of such apps will further increase inequality.

There are a number of reasons that explain why not everyone can use a tracking app. In some cases, some people cannot afford to own smartphones. In other cases, some people cannot constantly carry with them such devices. This problem is compounded by the fact that some members of the most vulnerable populations, in particular, the elderly or the very poor, as well as children, are among those least likely to possess a device from which to download the app. In addition, not every single smartphone is suitable for downloading tracking apps like *Immuni*, and those that are not suitable tend to be the phones that are most affordable. As a consequence of these various factors, tracking apps' benefits are very likely to be distributed in an unequal way amongst the population. According to Floridi (as cited by Klar et Lanzerath, 2020), this factor "could deepen the digital divide" (page 3), that is to say, the discrepancy that exists between those who have access to technological means of information and communication and those who are excluded from the realm of technology, either for geographical or socio-cultural reasons.

It is important to note that this concern is not only about the unequal distribution of the benefits of tracking apps. It is also a concern about their effectiveness. Directly to this point,

Rothstein (2020) raises some doubts concerning the effectiveness of tracking apps; in particular, he mentions lower-income people, who seem to be mostly "at risk for COVID-19 but less likely to have smartphones" (page 1375). If that is right, the concern is that the apps will not be able to achieve their purpose. Furthermore, as mentioned above, there is an issue of inequality. Rothstein (2020) notes that the fact that lower-income people are less likely to have smartphones would mean that the reliance on tracking apps would create inequities within certain contexts, such as "employment, housing, or access to health care" (Rothstein, 2020, page 1375). In a similar way, Hart et al. (2020) argue that rural or semi-urban areas do not generally have high-speed Internet distribution and, as a consequence, the Bluetooth or GPS signal of the smartphone of people living there may not be sufficient or consistent. It follows that if we rely on tracking apps rather than more traditional methods of tracking, "we may have a situation where the virus can more easily get a foothold in certain communities, further increasing existing inequalities and creating an atmosphere of stigma and disparity" (Hart et al., 2020, page 30).

Exactly because I perfectly acknowledge these very important points, I argue that, for those who do have a smartphone, downloading the *Immuni* app should be the default option. As a matter of fact, I maintain that, in such a critical situation, especially in light of the worries about inequalities, people who do have the benefit of possessing a smartphone have even more reason to do their part to accelerate the entire process of Covid-19 recovery by using tracking apps. In fact, people who can make a difference in this way can provide significant benefits not only to themselves but also to others, including those less fortunate. I recognize, of course, that it is unfortunate that not everyone can personally make use of tracking apps. Tracking apps are not best seen as something that would create additional inequalities, however. Importantly, in the end,

everyone can benefit from this kind of solution. The more people who can use the apps do use them, the less likely everyone, including those less fortunate, will be exposed to the virus. Further, it is important to take account of the fact that the *Immuni* app is free of cost and, since it is based on Low Energy Bluetooth, its impact on the smartphone's battery is very minimal. *Immuni* does not even require one to keep one's device connected to the Internet connection on all the time: the only thing that matters is the Bluetooth signal.

Hence, I argue that far from increasing inequality, the use of tracking apps is likely to decrease inequality. Furthermore, the widespread use of such apps is a realistic possibility at least in Italy where the majority of the population lives with their phones in their pockets, bringing them everywhere as if they were precious jewels. By simply keeping the Bluetooth signal of our smartphones on and checking for *Immun*i's notifications, just like we check for emails or social media notifications, we can have an enormous impact for the good: such actions are almost certainly going to help maximize the overall wellbeing of our society which, in this current Covid-19 pandemic, must be a priority.

Furthermore, it might be helpful to take account of the fact that social distancing and national lockdowns, which represent the two most common methods used so far to fight against the pandemic, are far more likely than tracking apps to increase inequalities. In fact, while for financially-stable people to work remotely or to temporarily suspend their economic activities may be quite disturbing, the situation is far worse for people "who cannot work remotely, do not have paid sick leave, or do not have savings" and for whom mass quarantines are synonyms for "destitution and despair" (Goodman, 2020, page 1). Of course, the consequent bad psychological costs on these people's mental and physical health are undeniable. As many studies show, the most

widespread psychological disorders associated with isolation and quarantine are emotional disturbances like insomnia, depression, nervousness and sadness. In particular, “low mood and irritability stand out as having high prevalence” (Brooks et al., 2020). That said, I see this reason as a very powerful one to move away from a primary reliance on the practice of social distancing and widespread lockdowns to the use of tracking apps. Goodman is absolutely right that this would “allow for geographically targeted, appropriately scoped quarantines that minimize additional hardships for society’s most vulnerable communities” (Goodman, 2020, page 1). On balance, then, we see yet again that the benefits associated with the use of tracking apps such as the *Immuni* app to combat the spread of Covid-19 outweigh the costs, even when we focus on worries about the unequal distribution of benefits.

6. State of Exception

So far, I have mentioned the concept of a "state of exception" quite a few times in order to support my argument. What do I exactly mean by that term, however? What are the main characteristics that make a particular situation one of exception? The state of exception has been widely analysed and discussed by philosophers such as Carl Schmitt (1927) and Giorgio Agamben (2005). Basically, it can be defined as "the sovereign's ability [under very specific circumstances] to transcend the rule of law in the name of the public good" (Vidal, 2020, page 1). The state of exception usually gets activated whenever the community is facing a dangerous risk which needs to be quickly and successfully solved. For this reason, the government is somehow justified in temporarily introducing one or more exceptions to current rights, such as the right of freedom or that of privacy. Another important feature of the state of exception is represented by the government's recognition of "the enemy" (either physical or not) which has to be eliminated or at least somehow reduced. The state of exception applies to all people in an equal manner, meaning that it goes beyond citizens' wealth, moral status, religion or gender. We can therefore assume that the unprecedent and threatening situation itself makes the exception possible, and prioritizing safety becomes the most important reason to bring about the state of exception. Finally, the state of exception has always been a core component of politics and law because, as I have previously explained, it involves going beyond the established and existing legal order (which proves to be inefficient in certain situations) in the name of and for the sake of public good.

It is important to highlight the fact that, politically speaking, the state of exception is neither an *état de guerre* nor an *état de siege* (Preston et al., 2014, page 438). In fact, while the first refers to a situation in which "civil and military authority act in concert" (Preston et al., 2014, page 439), the second one refers to a situation where the military authority assumes the major role. The state of exception, instead, implies some sort of suspension of constitutional rights and the establishment of emergency powers. More precisely, Agamben (as cited by Preston et al., 2014) defines the state of exception as a "zone of indifference", where the distinction between " 'law' and 'non-law'" (page 439) is blurred.

A recent example of a context in which the state of exception has been adopted was after the terroristic attack to the Twin Towers in New York City on September 11, 2001. Following that occurrence, a range of security measures and extensive monitoring procedures were established in order to guarantee what the US government called the "national security". For instance, many strategies were used in order to keep track of people's movements and contacts; for example, the government was able to monitor public spaces through technologies such as cameras, and to analyse people's private messages, databases and telephone calls. What emerges, therefore, is that certain rights were treated as less important, especially if we think about the population's overall safety. To be sure, people may reasonably maintain that in some instances the United States government went too far after the September 11 terrorist attack. Surely, though, reasonable people can agree that in the immediate aftermath of these attacks, when it remained unclear whether the chain of attacks would continue, the government was justified in the name of the public good, to act quickly and to put into place security measures—even ones that may have temporarily suspended some rights. If this example does not persuade, think of the case of a natural disaster.

In circumstances such as a widespread forest fire, a volcanic eruption, or a hurricane, it is often not only reasonable but required that certain rights are curtailed for the public good.

We can draw a parallel between these particular emergency cases and that of Covid-19. However, although also here technological means of surveillance quickly became widespread, the type of "enemy" which the US wanted to fight against was human and physical (that is to say terroristic groups); indeed, in our current situation, things get complicated because our most hardened enemy is the invisible virus which keeps running very fast and overcomes every kind of obstacle or barrier. Numerous people are dying, and this seems to be precisely the sort of case in which the government has a responsibility to act quickly and efficiently in the name of the public good—even if this means, at least temporarily, placing less importance on or even suspending certain rights.

Some people might be tempted to argue that the current Covid-19 crisis does not, after all, qualify as a state of exception. They might argue that also other forms of viruses (like the seasonal flu which is quite common, especially during winter times) have pretty much the same effects and consequences, such as infections and, although very rare, deaths. However, the term *pandemic* itself (the Greek word *pándēmos* refers to something that touches upon all people, an entire crowd) already suggests the intensity and the gravity of this current situation: the Covid-19 virus is currently and rapidly spreading all around the continents, simultaneously affecting extremely high numbers of people. This is the reason why I believe that this current situation can be definitely considered one of exception: not only is it very risky because characterized by thousands of worldwide infections and deaths per day, but it could be also possibly solved by momentarily rejecting, suppressing or decreasing some type of rights.

After this brief explanation of the state of exception, I wondered how people may feel while living in or dealing with a state of exception and what could drive them to accept technologies such as tracking apps. Wnuk et al. (2020) argue that one of the strongest motivations people may have is represented by "the pursuit and maintenance of personal control" (page 3) which the Covid-19 pandemic has seriously undermined. As a matter of fact, Covid-19 appears to be something which is out of our personal control and, consequently, is seen as a minacious threat not only to our own existence but also to that of our relatives or beloved ones. Being this current one such an exceptional and unprecedent type of situation, what emerges is a huge and "generalized sense of uncontrollability" (Wnuk et al., 2020, page 3) which we may reduce by relying on institutional and governmental norms. In fact, if we follow the *compensatory control model* (Wnuk et al., 2020), we acknowledge that the more people feel threatened (and, consequently, insecure because their sense of control tends to decrease), the more likely they are to accept governmental control. On a more specific note, "by adhering to those in power and those with agency" (Wnuk et al., 2020, page 3) people hope to gain, at least in part, some sort of control over their own lives. And, of course, this could push them to accept the use of tracking apps which are very likely to be perceived as successful tools to fight against the pandemic.

The second significant human motivation that Wnuk et al. (2020) mention is the perceived realistic threat of Covid-19, which is strongly related to the one I have just talked about. However, I see it as an even strongest reason that may lead people to use tracking apps, because the possibility of being infected is high and nobody can be said to be immune. Plus, we all want ourselves and our loved ones to be safe and protected against the virus. In this regard, Wnuk et al. (2020) refer to previous studies that had been performed (primarily within the context of terrorist

attacks) to examinate the effects of perceived threats on people's disposition regarding civil rights; what emerged was that "people under threat are more likely to accept restrictions on democratic procedures and to exchange their rights for security" (Wnuk et al., 2020, page 4). For instance, acknowledging that a relative or a loved one may die in a terroristic attack correlated positively with increased support "not only for stricter methods for dealing with terrorists, but also for the harsher punishment of social norm breakers, increased surveillance and limiting the freedom of speech" (Wnuk et al., 2020, page 4). Overall, we can conclude by saying that the higher the level of personal threat associated with Covid-19 is, the greater support surveillance technologies like tracking apps may receive. Again, what we need to point out is that this is a temporary and exceptional kind of situation in which people may feel highly threated by external agents and, for this reason, may be more likely to accept extraordinary governmental measures aimed at protecting their safety.

7. Utilitarianism

I have defended the use of developing technologies, such as tracking apps, in the context of public health crises such as the current Covid-19 pandemic by relying primarily on the ethical theory utilitarianism. Utilitarianism is roughly a view according to which we can determine the ethical significance of any action by focusing on its consequences. To put it in a very simple way, we can say that if an action, a policy or a law brings about the *best* consequences, which maximize, for example, utility, overall wellbeing or happiness, that action is right; on the other hand, if an action brings about the *worse* consequences, that is to say whatever is not pleasure and freedom from pain and suffering, that action is wrong.

Utilitarianism traces its roots back to the nineteenth-century England and was born out of the ideas and thoughts of two early utilitarians, Stuart Mill (1806-1873) and Jeremy Bentham (1748-1832). Since they were witnessing many injustices and unnecessary pain around the society they were living in, the two philosophers began to challenge the institutions of their days, which were responsible for tremendous suffering and inequality of treatment. In particular, they called for several socio-political changes by appealing to utilitarian principles; for example, they wanted to put an end to slavery and to the bad treatment of animals, supporting the wrongness of such actions. Further, they underlined the importance of establishing universal suffrage and equal rights for women. In brief, these early utilitarians argued that society should focus on benefiting rather than harming the general wellbeing; in their opinion, everyone's happiness and wellbeing matters in the same way, and no one should be prioritized (Driver, 2014).

Utilitarianism can be seen as the combination of three main ideas. First, utilitarianism is a variety of consequentialism. This is a theory of rational action which defines that what is right or wrong is whatever brings about the best consequences, meaning that we should judge actions and states of character in terms of how they affect the goodness or the badness of the lives of those involved. This principle, which takes into account all the kinds of value possible, should be valid not only now, but also in the future. So which kinds of value matter? Contemporary utilitarians disagree about this. Traditionally, utilitarians are hedonists and, as such, sustain that the only thing that is good-in-itself or the sole ultimate form of intrinsic non-moral value is happiness, which basically coincides with a state of pleasure and freedom from pain and suffering. Even traditional utilitarians generally take into account various qualities of happiness, however, with the sorts of happiness available to beings through intellectual pursuits or from relationships being given more weight. Some utilitarians focus more on what we might characterize as informed preferences, these are the preferences we would have if were to be fully informed or more widely experience, if we were more rational and reflective. So this is the second component of utilitarianism, the theory of value. Finally, the third component of utilitarianism is the answer to the question: Whose wellbeing or happiness matters? Utilitarianism includes an *impartiality* principle according to which we must count everyone's happiness in the same way, without favouring or preferring any particular group of people.

That said, how do utilitarians elaborate their decision procedure? How do they decide about what is right or wrong? Contemporary utilitarians defend various approaches to what constitutes a right action and how to decide what is the right action. Probably the two most significant today are so-called act-utilitarianism and rule-utilitarianism. Act-utilitarians tend to insist that we must focus

on each individual act and perform a sort of "cost-benefit" analysis, by listing all the potential costs and benefits of any particular action, figuring out the value of each cost and benefit and finally doing what has the *best* benefits at the *least* cost (in terms of suffering). Rule-utilitarians suggest that we should rather focus on a set of rules the general adoption of which is likely to bring about the best consequences. So here again, we would under a kind of "cost-benefit" analysis, but one that focuses on general rules rather than on specific acts. I adopt a sort of broadly act-utilitarianism, but a careful defence of this goes beyond the scope of this project. Furthermore, it should be clear that if we focus on particular actions or on general rules, either way, on utilitarian grounds, I believe I have shown that we have compelling reason to treat the current pandemic as a sort of state of exception and certainly compelling reason to put aside any potential privacy concerns for the sake of the greater good that can be achieved by using tracking apps (Sinnot-Armstrong, 2019).

Note, however, that clearly what we must focus on are the *likely* consequences, which are the consequences that our actions are likely to bring about. This means that if it brings about the best consequences and "maximizes overall wellbeing" (Goodman, 2020, page 1), the action is right; on the other hand, if it brings about the worse consequences, the action is wrong. However, one question remains: since we cannot predict the future, how can we tell the likely consequences? One method for doing so is by relying on information gathered from surveys or on results from scientific studies (Prof. Annette Bryson, 2021).

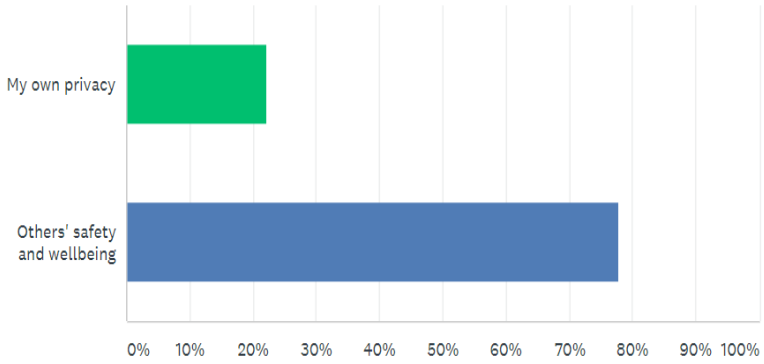
Given this brief explanation, how can we apply it to our Covid-19 specific context? Put it in a very simple way, "the public health benefit of the tracking apps practice outweighs the potential harms to individual rights" (Goodman, 2020, page 1). This means that what would be

maximized is public health and overall wellbeing because through the massive use of tracking apps, the situation would be much easier to control and the benefits would be many. Of course, we should consider the costs as well, including possible privacy violations. However, what I have sustained so far is that, in this particular and unprecedent type of situation, we ought to "choose the course of action which maximizes utility compared to the alternatives" (de Hoven, 2010, page 69). Furthermore, despite a few risks with doing so, I argue that, on balance, the ethical reflections count in favor of making the use of the Italian *Immuni* app legally obligatory.

In this regard, I would like to briefly mention a short survey I have conducted (on *Survey Monkey*) in November 2020, in order to analyse the reaction to the *Immuni* app of young people in my community. Although the sample was pretty small, the answers given by the participants proved to be in support of my argument. More specifically, the respondents were 36 (both men and women) and the medium age was 20 years old. What emerged from the results was that more than 20 people were "likely" to download the *Immuni* app, and only 3 out of 36 declared to be "very unlikely" to download it. In addition, 77.78% (meaning more than 28) of the respondents thought the app will prove to be useful and, therefore, were more willing to use it. However, the answers that are most significant to my study are the last two; one is "Would your privacy be a concern for you when it comes to downloading the app?", and the other is "Would you value more your own privacy or others' public safety and wellbeing?". And the results were quite surprising. As a matter of fact, for the first question, 63.89% of the participants chose the option "no", and for the second one, almost 80% stated that they would prioritize others' safety and wellbeing *rather than* their own personal privacy (as shown below).

Would you value more your own privacy or others' public safety and wellbeing?

Answered: 36 Skipped: 0



ANSWER CHOICES	RESPONSES	
My own privacy	22.22%	8
Others' safety and wellbeing	77.78%	28
TOTAL		36

Further, among the most common explanations to the answers given, people said that in such an unprecedent moment, public health and wellbeing should be the most important priorities. In order to justify their answers, most respondents appealed to both personal moral values and to religious principles, according to which helping each other (especially in this time of need) is seen as one of our most fundamental obligations. What I found particularly surprising was that many participants considered *Immuni* quite similar to other types of apps (such as *Tik Tok*) and, consequently, do not see it as much dangerous. Indeed, as I said before, *Immuni* does not collect personal data while platforms such as Facebook or Instagram do, so *Immuni* could be said to be even safer. In the end, what mostly emerged from my survey is that relying on technology seems

to be the most appealing solution to slow the spread of Covid-19. Overall, the results of my survey, although very restricted, seem to sustain my utilitarian argument.

8. Conclusion

In this thesis, I have argued that, despite some technical and moral challenges that may arise, the use of digital contact tracing (in particular of the Italian app *Immuni*) represents one of the best solutions in the fight against the spread of Covid-19. Of course, in order for it to be effective, *Immuni* should be used by as many people as possible. This is the reason why I sustain that the use of *Immuni* should be made legally obligatory. As shown in this thesis, the *Immuni* app has been developed in a way that does not largely invade one's personal privacy and, moreover, is for free. Plus, if we think that nowadays technology has become an integral part of our lives, I claim that using it for a useful purpose (namely, to reduce the social, psychological and economic consequences that Covid-19 brings about) is quite a secure and effective approach.

In order to sustain my argument, I relied upon utilitarianism, according to which what needs to be maximized is overall wellbeing and public safety which, in such an unprecedent and exceptional situation, is certainly what matters the most. Of course, I also took into account some possible counterarguments, including privacy and the inequality factor. Concerning the first, I have argued that the use of *Immuni* should not be seen as a way for the government to control citizens' movements and contacts, but instead as a positive way to monitor and somehow reduce the circulation of the dangerous virus. Further, I have underlined that not everyone can afford the use of *Immuni*, either because of the lack of a mobile device or because the device is too old. However, exactly because of these reasons, I sustain that for those who have the opportunity to positively contribute to public health by simply keeping the Bluetooth signal on, downloading *Immuni* should be the default option.

To conclude, I would like to highlight once again the useful contribution that technology is able to give to our society, especially in this period. Although we need to carefully analyse its pros and cons, I argue that, in the Covid-19 exceptional state, general wellbeing is definitely more important than some possible violations to our rights. As shown throughout my entire thesis, relying on *Immuni* would be optimal and would allow each of us to slowly go back to our previous "normal" life while, at the same time, to avoid additional economic crises and to slow the spread of Covid-19.

Bibliography

Abbas, R., & Michael, K. (2020, April). *The coronavirus contact tracing app won't log your location, but it will reveal who you hang out with*. The Conversation.com. Retrieved February, 2021, from https://theconversation.com/the-coronavirus-contact-tracing-app-wont-log-your-location-but-it-will-reveal-who-you-hang-out-with-136387.

Akhlaghi, F. (2020, July). *Guest Post-Pandemic Ethics: Your Freedom Really Matters. So What?*. Practical Ethics.

Amato, Rosaria (2021). *Istat: a dicembre 101 mila lavoratori in meno, 99 mila sono donne*. La Repubblica.it. Retrieved February, 2021, from https://www.repubblica.it/economia/2021/02/01/news/istat-285381015/.

Brooks, S., & Webster, R. (2020, February). *The psychological impact of quarantine and how to reduce it: rapid review of the evidence*. TheLancet.com. Retrieved April, 2021, from https://doi.org/10.1016/S0140-6736(20)30460-8.

Chan, J., & Foster, D. (2020, May). *PACT: Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing*. Allen School of Computer Science & Engineering, University of Washington. Retrieved April, 2021, from arxiv:2004.03544v4.

Cranor, L. (2020, November). *Digital Contact Tracing May Protect Privacy, But It Is Unlikely to Stop the Pandemic*. CACM, Volume 63, Issue 11. Retrieved March 2, 2021 from https://doi.org/10.1145/3423993.

Davies, D. (1997). *The relationship between science and technology in the primary curriculum - alternative perspectives*. The Journal of Design and Technology Education, 2.

Davisson, A., & Booth, P. (2016). Introduction to *Controversies in Digital Ethics*. In A. Davisson & P. Booth (Eds.). *Controversies in Digital Ethics* (pp. 1–9). New York: Bloomsbury Academic. Retrieved May 1, 2021, from http://dx.doi.org/10.5040/9781501310553.0006

Den Hoven, J. (2010). The use of normative theories in computer ethics. In L. Floridi (Ed.*), The Cambridge handbook of information and computer ethics* (pp. 59-76). Cambridge University Press.

Den Hoven, J., & Warnier, M. (2020). "Privacy and Information Technology". The Stanford Encyclopedia of Philosophy. Edward N. Zalta (ed.). Retrieved October, 2020, from https://plato.stanford.edu/archives/sum2020/entries/it-privacy/.

Driver, J. (2014) "The History of Utilitarianism". The Stanford Encyclopedia of Philosophy (Winter 2014 Edition). Edward N. Zalta (ed.). Retrieved April, 2021, from https://plato.stanford.edu/archives/win2014/entries/utilitarianism-history/.

FreeDictionary. *Privacy*.

Goodman, B. (2020, April). *Guest Post: Pandemic Ethics. Social Justice Demands Mass Surveillance: Social Distancing, Contact Tracing and COVID-19*. Practical Ethics.

Hart, V., & Siddarth, D. (2020, April). *Outpacing the Virus: Digital Response to Containing the Spread of COVID-19 while Mitigating Privacy Risks*. Harvard University: Center for Ethics.

Klar, R., & Lanzerath, D. (2020). *The ethics of Covid-19 tracking apps-challenges and voluntariness*. Research Ethics, Volume 16, 3-4. Retrieved October, 2020, from https://doi.org/10.1177/1747016120943622.

Naccarato, T. (2015). *Alunni ciechi e ipovedenti: tecnologie informatiche e software a supporto della didattica*. Disabili.com. Retrieved March, 2021, from https://www.disabili.com/scuola-a-istruzione/articoli-scuola-istruzione/alunni-ciechi-e-ipovedenti-tecnologie-informatiche-e-software-a-supporto-della-didattica.

Nissenbaum, H. (2004). *Privacy as contextual integrity*. Washington Law Review, 79, 119-157.

Nissenbaum, H. (2010). *Privacy in Context, Technology, Policy, and the Integrity of Social Life*. Standford University Press.

Olson, P. (2020, May). *Don't Stand So Close to Me: AI Cameras Police Social Distancing at Work*. Wall Street Journal (Online). Retrieved November, 2020, from https://www.wsj.com/articles/dont-stand-so-close-to-me-ai-cameras-police-social-distancing-at-work-11589452202.

Peterson, J., & Chadderton, C. (2014). *The 'state of exception' and disaster education: a multilevel conceptual framework with implications for social justice*, Globalisation, Societies and Education. Retrieved April, 2021, from 10.1080/14767724.2014.901906.

Prof. Bryson, A. (2021). John Cabot University, personal interview.

Richterich, A. (2018). *The Big Data Agenda: Data Ethics and Critical Data Studies*. Pp. 71-90. London, University of Westminster Press.

Rothstein, M. (2020, June). *Public Health and Privacy in the Pandemic*. AJPH, Volume 110. Retrieved March, 2020, from https://doi.org/10.2105/AJPH.2020.305849.

Sandler, R. (2013). *Ethics and Emerging Technologies*, Palgrave Macmillan.

Scoglio, S. (1998). *Transforming Privacy: a Transpersonal Philosophy of Rights*. Greenwood Publishing Group.

Solove, D. (2014, January) *10 Reasons Why Privacy Matters*, Privacy+ Security Blog. Retrieved March, 2021, from https://teachprivacy.com/10-reasons-privacy-matters/.

Sorgner, S. (2021). *We have always been Cyborgs. Digital Data, Gene Technologies and an Ethics of Transhumanism.*

Sinnott-Armstrong, W. (2019). "Consequentialism", The Stanford Encyclopedia of Philosophy (Summer 2019 Edition). Edward N. Zalta (ed.). Retrieved April, 2021, from https://plato.stanford.edu/archives/sum2019/entries/consequentialism/.

Stoops, T. (2020, April). *Managing health privacy and bias in COVID-19 public surveillance*. CE Think Tank Newswire. Retrieved November, 2020, from https://www.brookings.edu/blog/techtank/2020/04/21/managing-health-privacy-and-bias-in-covid-19-public-surveillance/.

Vidal, E. (2020, June). *Carl Schmitt and International Politic*s, backstagepolitics.com. Retrieved March, 2021, from https://backstagepolitics.com/carl-schmitt-and-international-politics/.

Vitak, J., & Zimmer, M. (2020, September). *More Than Just Privacy: Using Contextual Integrity to Evaluate the Long-Term Risks from COVID-19 Surveillance Technologies*. SM+S. Retrieved February, 2021, from https://doi.org/10.1177/2056305120948250

Warren, S., & Brandeis, L. (1890, December). *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5, pp. 193-220.

Wnuk, A., & Olesky, T. (2020, September). *The acceptance of Covid-19 tracking technologies: The role of perceived threat, lack of control, and ideological beliefs*. PLos ONE 15(9). Retrieved December, 2020, from https://doi.org/10.1371/journal.pone.0238973