HUMAN TECHNOLOGY
FOUNDATION

TECHNOLOGY GOVERNANCE IN A TIME OF CRISIS

COVID-19 RELATED DECISION SUPPORT

CONTENTS

This report does not constitute legal advice and is provided for information purposes only.

FOREWORD

In our collective psyche, epidemics are one of the evils that threaten our existence. The COVID-19 crisis has shown, vividly and abruptly, that an epidemic can also disrupt society and paralyze the world economy. In this challenging situation for public policy-makers and business leaders, technology is clearly a valuable asset, both for combating the pandemic and for reopening society in the medium term. The roles played by IT-based responses also raise ethical questions.

In keeping with its mission, at the request of its partners, the Human Technology Foundation undertook this study to determine how, in the current context, technology can still be used to benefit humanity. The study was led by a steering committee chaired by Jean-Louis Davet, Chief Executive Officer of Denos Health Management.

The work was carried out according to the Foundation's signature method, bringing together international, multidisciplinary experts, namely specialists in the target technologies, lawyers and ethicists, supported by the teams in our Paris and Montréal offices.

We collaborated with researchers from the International Observatory on the Societal Impact of AI and Digital Technology (OBVIA) and instructors/researchers from several universities located in Montréal, Lille, Sherbrooke and Namur. Also taking part were member lawyers of ITechLaw and staff from partner companies such as Samsung and EY. The study was supported by institutions such as the Chambre de la sécurité financière du Québec and the Mutualité Française.

I would like to thank the thirty or so experts who rose to the occasion and contributed their skills, particularly the members of the steering committee and coordinating team.

Beyond the current crisis, we hope that the method developed and set out in this report will be of use in selecting and governing IT-based responses to this new situation, which is likely to remain with us for some time.

We hope you find our report rewarding.

Eric Salobir
Executive Committee Chair
Human Technology Foundation

INTRODUCTION

NEVER BEFORE HAS A PANDEMIC SPREAD ACROSS A WORLD SO ABUNDANT IN TECHNOLOGIES AND DATA. WHILE NOT ENABLING ALL COUNTRIES TO SUFFICIENTLY ANTICIPATE THE IMPACT OF COVID-19 FROM ITS ONSET, THE **POWER OF DIGITAL TECHNOLOGY HAS BEEN LEVERAGED UNIVERSALLY** TO ACCELERATE SCIENTIFIC RESEARCH, LIMIT THE SPREAD OF THE EPIDEMIC AND NOW FACILITATE THE REOPENING OF BUSINESSES.

However, use of this significant power can also present its own risks and raise concerns that may even slow the adoption of proposed solutions. Often caught up in a tangle of constraints or contradictory orders, public and private decision-makers are faced with choosing between the lesser of two evils. In particular, the **effectiveness of health measures, safeguards for individual liberties, digital sovereignty, social inclusion** and **widespread adoption** of the proposed measures are the issues at stake.

Citizens are questioning politicians on the social impacts of the health and IT-based systems they are considering. Businesses are turning to the authorities for concrete recommendations to follow and guidelines defining their responsibilities. Employees are challenging their employers about how real their commitments are to social responsibility and workplace safety. Governments are calling on various intermediary bodies that can facilitate adoption of the measures they recommend, without actually imposing them. And businesses are also trying to assess the ways and means available to promote the buy-in for protective solutions among their employees. Customers are challenging the right of a store owner to oblige them to take a particular action to enter the store, or even to benefit from special conditions. So many different situations! So many ethical beliefs and values tossed around by all and sundry, on either side of the fence. In the end, they are all **dilemmas** and **constraints** for those who have to decide on or manage the implementation of IT-based health protection measures.

This report and its proposed methodology are primarily addressed to such decision-makers. This approach aims to provide them with the means for analyzing and deciding on the use of technologies to safely exit the crisis and accelerate a healthy return to normalcy. This report can be read on two levels: the first addresses decision-makers across all types of organizations and governance bodies, and the second is more specifically geared to businesses.

Developed during the COVID-19 crisis, the proposed method in fact heralds a more general approach (which will be the subject of future work) for implementing algorithmic and personal data processing, whose adoption and proper use involve fundamental ethical considerations.

This approach can be naturally extended to **other areas of healthcare**, where the crisis has catalyzed underlying existing trends, paving the way for increasingly digital and data-intensive health services. Even more broadly, this method could be adapted to **make ethics an enabler and not a constraint** for developing digital services whose sensitive nature requires a contextualized approach in our democratic societies.

Our proposed **methodological approach** consists of several stages:

- Setting up an appropriate **governance body**, which brings together all stakeholders and steers the project from design stage through completion (return to "normal" health conditions), and has technical, ethical and legal expertise.
- Building a **single frame of reference**. Often-used analogies to familiar situations (plague,

war, terrorism, mass surveillance, etc.), conjure up images and mould our perceptions of the situation. Some biases cause decision-makers to prefer certain solutions while others trigger rejection or opposition from those the solutions are intended for. Clearly, the choice of mindset is key. Among other things, it helps build a shared vision of the issues at stake.

- **Clear identification of needs** (tracing individuals carrying the virus, studying community behaviour, monitoring compliance with health measures, controlling access to private spaces, etc.), taking into account the **overall health system** in which an IT-based solution is to be used.

- In-depth analysis of available technologies and the technical, safety, ethical and legal issues related to deploying them.

- Based on the foregoing, a **decision-making process** should be rolled out **using a multifactor matrix** that involves all project stakeholders. The considerations incorporated in this process will make it possible to identify risks and understand how to mitigate them, pave the way for broad adoption of the chosen measures, and determine the governance conditions and how they should evolve over time.

This report is made up of three main parts:

- The first part focuses on the anthropological, social and ethical aspects related to the IT-based responses for exiting the health crisis. In particular, it discusses the different mindsets, principles and values conducive to achieving the crucial shared frame of reference mentioned above.

- The second part provides an **overview of the main technologies available** with regard to health, technical and societal issues. Particular attention is paid to the most impactful issues, such as the nature of the data collected, how the data are processed and stored (centralized/decentralized/hybrid), the security aspects related to the technology used, etc. This part also aims to **make the IT-based aspect understandable for decision-makers** from outside the industry.

- The third part sets out in detail the **methodology** and accompanying tools. It presents the multifactor impact matrix we developed and how it is used. The matrix is presented in its entirety in the appendix. **The method has been fully applied to a selection of responses illustrating the diversity of anti-COVID-19 IT-based solutions developed around the world.** Eleven solutions were analyzed in depth by an international team of experts in technology, health, ethics and law. **The results and lessons learned from this work are highlighted in the different sections of the report and inform our recommendations.** Appendices include a comparative table of these 11 responses, as well as summaries of the analyses carried out on each.

Jean-Louis Davet
President, DENOS Health Management
Senior Advisor Human Technology Foundation

CHAPTER 1

BACKGROUND AND PERSPECTIVES

Decision-makers, public and private, institutional and business alike, now find themselves facing a flood of opinions that raise issues of ethics around the IT-based health crisis solutions they are weighing. However, against the complexity of a pandemic, accepting every argument that claims ethical legitimacy would result in paralysis. **So it is essential to clarify which legal and ethical principles to favour.**

The **social acceptability** of a technology does not depend solely on its accessibility, effectiveness, explainability and easy applicability for a wide audience, or on the related technical, legal and ethical precautions. Our level of acceptability also depends on the mindsets we use to understand the unknown based on what we know. This crisis has led to a real **conflict of mindsets**. Decision-makers must determine what tone to take in the current situation, to enable adoption of the chosen tool and its contribution to achieving a desired outcome.

Every mindset can introduce its own **biases** when determining the measures to implement. Such biases influence both decision-makers and those directly affected by the implemented measures as they cause some to prefer specific solutions and others to reject or oppose them.

The mindset around **major epidemics of the past** such as the plague, cholera or AIDS conjure up images, leading us to overreact to or, conversely, downplay the seriousness of COVID-19. The mindset around **mass surveillance** prompts us to consider the use of technology as irreconcilable with safe-guarding individual freedoms. Clearly, other more enlightened mindsets must be used. Such a case in point is the mindset around our **relationship with nature**, which encourages us to develop a collective awareness of our shared responsibility in the current crisis. More specifically, the **mindset around care** implies that crisis exit strategies should be based on principles of inclusive governance, dialogue, solidarity and equity, accountability and trust. This seems to be the most constructive mindset. In particular, it avoids the pitfalls of other mindsets, such as around **war** and **terrorism** which, on the one hand, shift responsibility for defending ourselves to the state and, on the other hand, implies that the danger is external, while we can all be carriers of the virus and are therefore all partly responsible for the solution.

We all face danger from others and at the same time pose a danger to them. **The mindset around care calls for a continuous search for the right compromise between the need for freedom of choice for individuals and each person's responsibility for others, while paying particular attention to the protection of the most vulnerable populations.**

AMBIVALENT RELATIONSHIP WITH TECHNOLOGY

Amidst the urgency of the situation, a host of digital projects is now underway across the world in an attempt to find ways to address the dilemmas around SARS-COV-2 (COVID-19). The common challenge of these technological solutions is to trace the local, regional, national and international transmission and spread of the virus in populations in order to contain infections, find a way to get back to normal living and avoid a second wave.

These developments are a source of hope, as the use of innovative medical technologies and public health tools could provide effective means of combating pathogens. But using today's digital innovations is not without risks and raises important issues for society. Their misuse and the widening of their scope to purposes other than originally intended — whether by public authorities or private actors (police use leading to excessive controls, monitoring by employers, use by insurers, etc.) — require guarantees that the collection and processing of data comply with clear ethical and legal frameworks that protect individual rights and freedoms. Otherwise, they may profoundly undermine the public's confidence in the promoters of these projects, and thus jeopardize the social solidarity required to combat a pandemic.

The ambivalence of mankind's relationship with technology raises **practical questions** that are by nature at the same time **philosophical** (What can we learn through technology? Is the information reliable?), **ethical** and **legal** (What are the conditions for claiming certain benefits through the use of technology? What rules should govern its use? What are the risks and are they equitably shared?) and **political** (How do we govern the deployment and use of technology in a given society?).

PRACTICAL ETHICS TO GUIDE DECISION-MAKING

In an environment of fear, uncertainty and sometimes even suspicion, decision-makers now find themselves facing a flood of opinions that raise issues of ethics around the solutions they are weighing: **governments** over national measures, **employers** concerning solutions they could implement to protect employees; retailers and public transit for their **customers**; building **owners** for their **tenants**, etc.

Out of this context emerge issues that could lead to the rejection of every solution put forward and thereby to paralysis. And the polarizing debate around some of the most highly publicized aspects of combating COVID-19 makes gaining a bird's eye view of the bigger picture difficult. For example, while the arguments put forward by defenders of individual freedoms and privacy are undeniably relevant and fundamental, the concept of privacy by design does not, on its own, fully address the ethical issues raised by the implementation of technology-based solutions. So, the issue is to find the **right balance** between the goal of **public health (the right to health)** and the various **freedoms** impacted by confinement, such as freedom of **movement**, **assembly** and **expression**, as well as **privacy**, **fairness** and non-discrimination, which are guaranteed to citizens but which could be compromised by certain uses that data might be put to. In particular, while some applications may enable contact tracing by public health actors or employers, they may also lead to the stigmatization or social exclusion of already vulnerable populations, thus reinforcing pre-existing injustices and inequalities. For example, the issue of access to these digital devices — whether in terms of cost, equity or social acceptability — is more pressing than ever. While 80% of the population in France has smartphones, the penetration rate in India is only 30%, not to mention the distribution disparities within the population itself, depending in particular on age group or social background. In other words, these populations cannot benefit equitably from automatic tracing solutions based on having a smartphone.

Clearly, a **broader view of ethics** must be applied to the different measures being studied to explain them to the public (as **individuals**, but also as **groups** or **communities**). The public must not be seen as mere **users** of digital tools: they are jointly responsible for the solutions to be implemented since they all share in creating the risk. A practical approach to ethics, without advocating any particular moral code must be understood as a thoughtful, open and hands-on initiative based on a genuine discussion of the values we wish for our society, for assessing, selecting and governing technological solutions to exit the health crisis.

TRANSITIONING FROM DISASTER MANAGEMENT TO LONG-TERM RISK MANAGEMENT

The fierce debates around IT-based solutions developed in the heat of the current health crisis highlight the real challenge for governance (for government agencies, industry, any organization and civil society), facing us over the long term.

On one hand, uncertainty remains high today with many questions unanswered — Will the virus mutate?; Can immunity be actually acquired and for how long?; Will seasonality affect the virus?; What is the potential for a second wave? Even if a vaccine does become available and, we hope, widely and equitably accessible to every single person on the planet, going forward we will inevitably face new epidemics that may take us just as much by surprise. On the other hand, our ability to mobilize the power of technology and harness digital expertise to prevent epidemics or protect our populations is a new and major asset for our societies in facing health disasters. But the methods for deploying these solutions will also come with their fair share of risk over the long term, particularly for regional, national and international sovereignty and the protection of user interests and freedoms. It is through constant exposure to these types of risks that we must learn to govern how we develop and implement solutions.

The processes for engaging stakeholders, analyzing and deciding on the best solutions, and facilitating ethical acceptance and social acceptability that will be developed to curb COVID-19 may offer the first outline of a governance model for the future. In such a future, technologies and algorithms along with extreme risks — health-related or not — will be determining factors and will be used to weigh our decisions in the light of overall ethical considerations.

SOCIAL ACCEPTABILITY OF TECHNOLOGY

The issue of ***access*** to technologies and their *social acceptability* is widely highlighted in the current debates around digital tracing technologies. These technologies (apps, smart watches, smart wristbands, etc.) could enhance and enable the return to social, economic and cultural activities. Very few studies have been conducted to date on the effectiveness of such technologies. One of them — extensively repeated since — stresses the need for adoption by a sufficient proportion of the population (around 60%, cf. *Big Data Institute, Nuffield Department of Medicine, Oxford University headed by Dr. Christophe Fraser*); if not, tracking their movements individually or collectively would be ineffective for monitoring the transmission of a virus nationally.

Since the effectiveness of these technologies depends on a high rate of voluntary uptake, a number of countries are now favouring more **traditional alternative tracing solutions** that have proved their worth in public health (telephone call centres, tracing by health personnel). The problem with this approach is that it is highly labour intensive and enormously time consuming. Given the historical underfunding of public health in many countries, the lack of adequately trained public health workers to carry out contact tracing is no surprise and renders an already lengthy process even more problematic. To illustrate these choices, public authorities are observing (Iceland, Singapore) or predicting (Belgium, France) an interest in innovative responses such as smartphone applications, as well as a lack of public support for digital tracing.

Interestingly, such lack of support is generally related to social, material, technology, or legal and ethical problems. Lacking either digital means or literacy, part of the population would not have the required technology, or would not have digital tools capable of supporting the proposed solution. Other causes cited relate to fears of mass surveillance or IT intrusion of privacy. These factors must of course be taken into consideration. But too few academic studies or media information sources to date have focused on the impact of the social myths and perceptions that filter our efforts to understand the current situation in Western countries. The social acceptability of a technology does not depend solely on it being broadly **accessible**, **effective**, **explainable** and easy to use (intuitive) for a wide audience, or on its related **technical**, **legal** and **ethical** precautions. The acceptability of digital tracing tools is also dependent on the value systems, and the mindsets we use to try to understand the unprecedented crisis based on what we are familiar with (we always try to understand the **unknown** based on the **known**), and on the value judgments around the technologies that these mindsets imply.

In other words, for example, making the interface of a tracing application user-friendly and intuitive, easier for a wide audience to understand and use, and demonstrating its usefulness, is no guarantee that it will be socially acceptable (i.e., find audience buy-in). Even ensuring full compliance in the design of the application with the main legal and ethical principles and values of a democratic society around the protection of individual rights is not in itself enough to guarantee that a technology will be widely used by its target audience. Why? Because our relationship with a technology is also mediatized by social affects and norms that influence how favourable we are to making it a part of our daily lives. Our **relationships** with IT-based tools are not "**pure**" (in the sense of purely functional or mechanical). Our relationships with technology are always coloured by emotion and idealizations. We adopt a technology that we see as acceptable, desirable or reassuring (for instance, perceived as not being a threat to our property, fundamental values and human rights).

A technology's social acceptability therefore does not depend merely on how effective, explainable, transparent, legally compliant and ethical, etc. it is. It depends also on the type of "background context" or "mind space" that colours this technology as more or less desirable and attractive or, conversely, undesirable within a given population.

UNDERSTANDING THE MINDSETS THAT SHAPE OUR THINKING

Our mindsets shape the way we understand and think about things. Collective sets of perceptions and social constructs play a major role in how we respond (accept or reject) to IT-based measures in

a time of crisis. We need to take a look at the main perceptions that make up the mindsets we use (more or less consciously) to gain an understanding of the crisis we are going through and the proposed solutions. In doing so, we can assess how suited or unsuited the mindsets are to the situation we are facing, and understand their effects on how we relate to the tracing technologies currently under debate. We can then adapt the **understanding and communication framework** to the current situation.

Without claiming to be comprehensive, we can identify at least five mindsets:

1. THE MINDSET AROUND PAST MAJOR EPIDEMICS
2. THE MINDSET AROUND WARTIME
3. THE MINDSET AROUND OUR RELATIONSHIP WITH NATURE
4. THE MINDSET AROUND MASS SURVEILLANCE
5. THE MINDSET AROUND CARE

It thus becomes essential for decision-makers involved in governance issues regarding innovative technologies to take into careful account the symbolic, cultural or perceptual conditions surrounding the social acceptance of a technology, if they wish to gain the trust and support of a target audience. Such conditions refer to the field of affects, beliefs and social perceptions. These meanings come from the interpretations that social groups (family, social network, association, business collective, particular population, group of populations, country, continent, etc.) give to a technology on the basis of their history (past experience), political engagement and culture (philosophical and religious beliefs, practices, arts, symbols, images, myths, stories, etc.) at any given time. These interpretations and the meanings they impose on a technology are not definitive. They can be refined and contested through counter-interpretations, changes to meaning, socially significant collective events that require new frameworks for understanding. We must keep in mind that these mindsets and the shaping of these **discourses will and probably must evolve through time and space**.

1 THE MINDSET AROUND PAST MAJOR EPIDEMICS

The mindset around past epidemics stirs our age-old fears and causes us to overreact, even if it means jeopardizing the economy and social relationships. In fact, COVID-19 is a global epidemic of viral origin. It thus shares a common range of meanings with other viral diseases (plague, cholera, AIDS, Ebola, Spanish flu). This has at least **three paradoxical practical consequences**. Because of its nature and unpredictable evolution, COVID-19 creates strong anxiety, fear and even fantasy. However, in view of the mortality statistics (e.g., 50 million deaths from the Black Death in the 14th century), the mindset around previous **deadly epidemic crises** relates to devastating pathogens, out of all proportion to the current pandemic crisis. This has led some to criticize the overreaction of governments that have imposed lockdowns, with unprecedented economic effects. Given this ambivalence, reactions vary widely, which explains the difficulty in predicting whether or not the public will support IT-based devices for tracking people carrying the virus. The concern is that much stronger because the mindset around major epidemics — at least in the West — does not naturally call to mind the new digital technologies, which did not exist in earlier historical instances. Therefore, until new technologies have demonstrated their **real effectiveness for public health** in the current crisis, social expectations of them will remain cautious. This lack of demonstrated effectiveness explains why many members of the public are reluctant to deploy tracing applications.

2 THE MINDSET AROUND WARTIME

The current crisis is also reviving memories of wartime deprivation and hardship. Leading politicians have intentionally linked the two situations to strengthen national unity in the face of COVID-19.


+11,00.00

For example, on March 16, 2020, during a message to the country, French President Emmanuel Macron announced, "We are at war." On May 8, 2020, the anniversary of the surrender of Nazi Germany, British Prime Minister Boris Johnson drew the same parallel. In an open letter to veterans, he likened the coronavirus pandemic to a "new battle" to be fought with "the same spirit of national endeavour" as 75 years earlier.

Summoning up the words and imagery of war draws on undeniable similarities between the two situations: the state of emergency, the call for national unity, the mobilization of health services, calling in the army, **mobilizing** all forces, controlling population movements (police control, IT-based monitoring), stocking up on essentials (pasta, rice, milk, flour...), closing borders, government requisitioning of equipment, war economy measures (redirection and nationalization of certain private activities for the purpose of combating COVID-19). The current crisis scenario does indeed resemble an exceptional wartime state of emergency, with restrictive measures affecting an entire country. But using the vocabulary of war is a double-edged sword, because it brings with it, in the present situation, its own interpretations of technology, not only as an arsenal and weapon of war, but also as a political-ideological means of controlling the public. That being said, are we really at war with COVID-19? Today's prevailing strategies do not so much resemble acts of war as gestures of diplomacy and caution, such as: limiting exposure to the virus, reducing interactions, self isolating, maintaining physical distancing, putting contacts on hold, communicating about channels of spread in order to contain it, wearing masks. Learning to live with SARS-COV-2 calls for arts other than the art of war: the art of **living together**, of **neighbourliness**, of circumspection, of **keeping the right distance** and of **consideration for others**.

By framing us in a paradigm of conflict, the mindset around war can make us lose sight of our relationship to others and our relationship with nature. In the current context of a health as well as a socio-economic crisis, wouldn't a less militaristic, more peaceful and calmer relationship with technology be more constructive? The mindset of war suggests that defending ourselves against an enemy is enough. And as a result, it risks minimizing the scope of the organizational changes that need to be made to contain the risk of epidemic.

3 THE MINDSET AROUND OUR RELATIONSHIP WITH NATURE

The current crisis is also bringing up questions about our relationship with nature. In fact, we are becoming collectively aware that economic activity without regard for the natural barriers and balances between species is one of the factors behind the current pandemic. Observers point to the speed with which SARS-COV-2 has spread around the world thanks to the globalization of trade. It has been found that the vast majority of COVID-19 victims were vulnerable owing to impaired health conditions (chronic diseases, respiratory diseases, obesity, smoking, etc.) resulting from lifestyle choices, socio-economic inequalities and industrial pollution. From this point of view, the primary cause of death is not SARS-COV-2, but rather in the way our lives are organized, which include disregard for public health recommendations, natural ecosystems, barriers between species, etc.

So **we are not primarily combating an external** enemy (nature, viruses are not foreign to us), but effects that we ourselves have caused. The war against nature mindset is therefore not relevant for discussing technologies whose objective is not to fight against nature. Unlike a future vaccine, which will give the immune system the means to destroy a virus, tracking technologies are not weapons of war against a natural scourge. Primarily, they are an "as far away as possible" means of prevention and protection against the virus.

The first step that this new mindset around our relationship with nature asks us to take is that **we become aware of our responsibility** for the current crisis. The second step involves, like our responsibility for **global warming**, a **profound transformation of social, economic and political organizations** at the international level. Determining how a chosen IT-based solution contributes to attaining a desirable future that we can share with our fellow citizens/employees requires a vision that gives meaning to the technology and the social actions it requires from its users.

4 THE MINDSET AROUND MASS SURVEILLANCE

There is another mindset that in the current crisis impacts, more directly and more strongly than the above mindset, the social acceptability of IT-based initiatives, particularly those using digital tracing: the mindset around mass surveillance. As soon as the first IT-based solutions for exiting the crisis appeared, a large number of prominent figures from the academic world and civil society entered the public debate to warn of the threat that any projects for digitally tracing population movements would pose to our democratic principles, the rule of law and fundamental freedoms. A direct consequence of the mindset around mass surveillance companies (as the recent cases of Snowden and Cambridge Analytica shows) is the polarization of the debate around privacy issues at the expense of other ethical issues.

Emphasizing the risks of possible abuses and the erosion of fundamental rights and freedoms that any use of digital technologies might entail is often backed up by one or two arguments that bioethicists, logicians and philosophers know well: the slippery slope and neo-Luddism.

The slippery slope theory holds that a given first step (the introduction of tracing applications), could (the realistic version of the reasoning), or — conversely — inevitably (the skewed version), lead to a chain of events culminating in a result that no one wants (the replacement of a democratic state with an authoritarian and repressive state, for example). This argument is misleading when it disregards that a set of democratic mechanisms can seriously reduce the risks of the proposed technologies going off the track: strict legal and ethical frameworks, external controls, ongoing user feedback, etc. The **neo-Luddite line of reasoning** holds that any plan to solve a human problem with technology would given priority to the technical solution over any more humane, social, political and ethical solution. This type of reasoning is also problematic because it presupposes that the IT-based tool could not be one means among many to a more global solution, as if the two were mutually exclusive, which is false.

The mindset around mass surveillance is linked to the legislative and political framework under which IT-based measures are deployed. In fact, implementation of any IT-based measures has to be (and will be) triggered by a state of emergency or special legislation to deal with the health crisis. In this context, many observers again use the slippery slope argument to warn against the likelihood of certain exceptional provisions sooner or later becoming the norm, albeit passed in an emergency situation. These observers base their warnings on past experience of states of emergency declared to deal with terrorism. They point out that special legislation had become enshrined in conventional legislation in those circumstances.

That being said, if, through the use of digital tracing tools, the fear of abusive curtailment of freedoms by governments or businesses is kept alive by the historical symbols it conjures up (totalitarianism, authoritarianism, etc.), this fear may, in some cases, be underestimating the strength of our institutional mechanisms (ethical, legal and political) to protect fundamental rights and freedoms. Since the second half of the 20th century, our democracies have developed solid democratic controls to protect against potential shifts in ideology that could undermine their foundations. While the risk of backsliding into repressive policies is always real, implementing stringent government surveillance in unprecedented times does not mean that we have abandoned our values and opened the door to all manner of abuses. Such cultural distortion also results in a reductionist interpretation of tracking and digital tracing. Tracking is not necessarily "threatening" or "bad".

Surveillance in the modern sense of the term emerged between the sixteenth and nineteenth centuries, before it was abused by the totalitarian regimes of the last century. It is no coincidence that the development of the term in the French language during this period coincides with the gradual birth of the rule of law. "Surveiller" was forged in the sixteenth century from the verb "veiller" which means "to stay awake (to intervene if necessary)", "to remain vigilant", and the prefix "sur" which indicates excess or superiority. "Surveiller" in this sense meant to "protect" something "smaller"

than oneself, to “keep it out of harm’s way”. Use of the verb became widespread in the eighteenth and nineteenth centuries, giving rise to the word “surveillance”, which appeared in English circa 1800. In the **positive sense** of the term (**watch over**), the function of surveillance is to guarantee a safe space. It is a **legitimate means** of ensuring public order and a duty enshrined from the outset in the rule of law, which must guarantee its citizens protection and the best possible conditions to enjoy their fundamental rights and freedoms.

The same nuances also apply to the means of surveillance: similarly, digital tracing technologies do not necessarily lead to **authoritarianism** or **totalitarianism**. In fact, carrying out surveillance by such means produces many social benefits. How many people in danger, stranded in the mountains or lost in an unfamiliar environment have been rescued thanks to telephone cell tracing or by activating the GPS on their smartphone?

Many crimes of various types have been prevented thanks to digital data. In certain situations, digital tracing can provide protection and rescue coverage unmatched in history. Under certain conditions defined by law, the potential for medical monitoring of patients and their state of health also offers exciting therapeutic possibilities in the field of personalized healthcare. Digital tracing tools give many athletes the means to measure their performance in real time, schedule tailored race training and evaluate their progress based on increasingly precise bio-physiological indicators. At city level, it can optimize the infrastructure planning based on analyses of crowd movement, road traffic, etc. But it is also true that digital tracing can involve many other possible spinoffs: invasion and loss of privacy, disclosure of personal data, covert unethical use of sensitive data, commercialization of health data, data theft, hacking of digital tools, stigmatization of certain segments of the population, abuse of power by public authorities, etc.

Given these different examples, digital tracing technologies can offer both the best and the worst, but there is no real cause and effect that they will inevitably compromise our future.

A political, legislative and ethical framework designed to protect democratic values and fundamental freedoms should provide effective protection against the risks of misuse of digital tracing technologies so that their disadvantages are minimized and their benefits maximized. To ensure that we move more towards improving the beneficial aspects of “surveillance” for both

individuals and the public (e.g., monitoring disease, influencing behaviour), we need an explicit and public social contract. Those under surveillance must be able to understand both the extent and the limitations of the surveillance, in order to accept it. Governments and businesses must do the same, and if necessary, limit certain types of surveillance that would be "effective" or "efficient" because they are not socially acceptable.

5 THE MINDSET AROUND CARE

As we have seen, a number of mindsets are used to view the crisis from a variety of perspectives and offer courses of action that reflect the perceptions identified. Some of these mindsets may seem more relevant than others. But the target that has been the focus of the vast majority of the public's hopes and efforts in the current situation lies elsewhere.

We are not really at war, faced with a defence issue where the enemy is at the borders, or putting the country's stability at risk. Nor are we in an anti-terrorism state of emergency, faced with a security issue where the enemy is linked to specific parts of the population, or certain profiles. Rather, we are in a situation where everyone is potentially both a risk and a resource for others, where everyone has to take responsibility for themselves and for others. Our present concerns, tied to the "total social fact" that we are currently experiencing (see Appendix 1), have not been prompted by unacceptable surveillance practices but by the spread of a pandemic and its multiple social, economic and political effects. Lastly, we are not engaged on the front line in talks with nature for a new alliance, as with the issues around climate change. Instead, we are dealing with a **public health issue** that involves safeguarding a common asset, namely health, which we are striving to maintain for as many people as possible, especially those of us most at risk of COVID-19 morbidity.

While the health emergency has similarities to other exceptional situations in terms of the means used, the end is nonetheless very different, as is the intent of the measures. Understanding this is essential if we wish to remain on topic, on vision, and on target. Faced with the pandemic as a public health issue, we are not at war, we are in a situation of care, and in need of care far beyond any other identifiable mindset, beyond any range of actions that may be parallel to, compatible with or complementary to our needs in the current situation.

Because the crisis underscores our fundamental **vulnerability** and **interdependence**. It brings to our conscious minds, through our confinement and its various consequences, that we all depend on the care and attention of countless private and public actors who, in every sphere of life in a society, enable us to go on living. The current situation underscores more than ever the value of "caring for yourself, others and the world", which transcends the bounds of private and public, and profoundly challenges the way we will carry on our human pursuits in the future: are we ready to do so with greater care?

It is important to stress here that while this call to care cannot be confined to the world of medicine and the unfailing commitment of our health care workers, even if they embody it, they are obviously part of it and play an essential role in managing the pandemic. **Reference to care in the crisis implies a much broader understanding of care, in which medical care is only one expression**, and is reflected in everything we would like to do (and are already doing) to make our "worlds" **livable** (worlds that includes our bodies, our social, cultural and technical environments, our relationship with nature), so that we can live and flourish in them to the fullest. In this sense, care is as much a goal as it is a set of subjective arrangements and particular practices whose purpose is to support, maintain, protect, and allow a human world, and all those who live in it, to flourish.

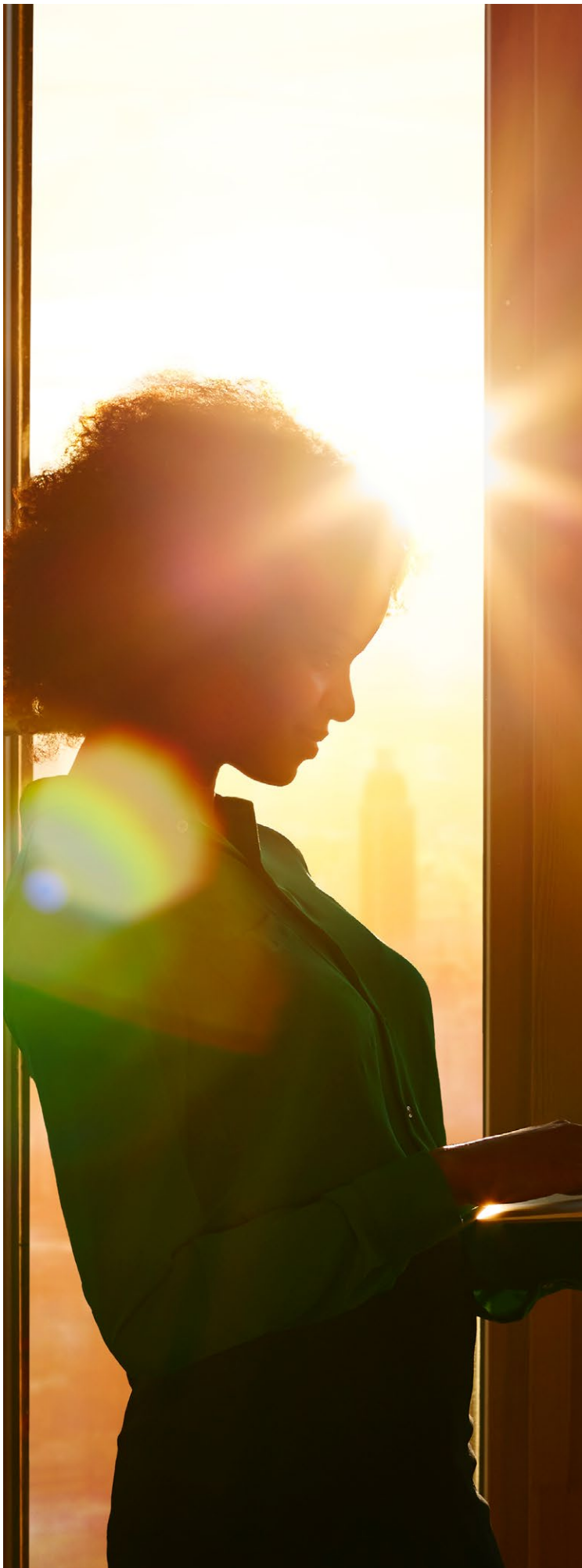
This need for care also ties in with a need for justice expressed by the public in the face of risks from new sets of inequalities and discrimination that crisis governance could create, in particular through recourse to certain tracing technologies in an emergency situation where the public is unprepared. **Finally, there can be no care policy without the inclusion and participation of all care stakeholders.** Concern for self, others and the world always presupposes the exercise of a set of skills that are always specific, often learned from experience and adapted to the challenges of specific situations (parental, social, educational,

environmental, cultural, etc.). These practices are themselves part of very diverse institutions, evaluation procedures, contracts of objectives, local policies and concrete cultures.

Beyond this exceptional period with its lockdowns and public health strategies implemented to avoid health system collapse in many countries, the mindset around care in the current situation calls more than ever for the development of an ambitious care policy and the conditions for a more just society. But care must not be limited to its biomedical sense, it must encompass much broader social, political and economic considerations.

A care ethic requires that those who aspire to it be transparent, sincere and consistent, which are necessary conditions for fulfilling any social contract, as well as for ensuring human dignity and human rights. Faced with the ever possible risks of breaking the social contract, compliance with a care policy requires not only a good **understanding of the technologies** proposed in the current crisis (Chapter 2 of the report), but also **inclusive governance** and an **appropriate technical, legal and ethical tool for assessing technologies** (Chapter 3 of the report). Indeed, any digital technology to support a crisis exit strategy should only be implemented on the condition that its design and use are subject to rigorous evaluation by independent bodies representing civil society, in accordance with processes that guarantee compliance of the technology with the terms of the social contract and democratic principles and values held dear by everyone faced with the crisis.

From the perspective of a crisis care policy, the ideal of inclusive governance and the multidimensional digital technology assessment tool discussed later in this report are complementary and necessary, which should be adapted to real situations on the ground, at the corporate, intermediary and government levels and in their interactions.



RECOMMENDATIONS

From a shared perspective of combating COVID-19 and resuming social, cultural and economic activities, this section, which focuses on the mindsets around the crisis, was an essential starting point. While the crisis poses many challenges, it has in fact shown that they also stem from a **conflict of perceptions**. Therefore, decision-makers and communities must be able to speak accurately about the problems encountered if they wish to find a tailored solution. To that end, it is essential to know **what mindset to appeal to**, what **tone to take**, and the consequences or implications (benefits and limitations) of such a choice.

In this current context where IT-based responses are sometimes equated by the public with monitoring and sometimes with war or terrorism, the question of **temporality** appears to be a crucial one for decision-makers. Governments must determine the criteria used to define a state of emergency, the conditions under which the exceptional crisis measures can be lifted and those that require the reactivation of exceptional measures to prevent a new epidemic. For businesses, the challenge is to ensure that practices for controlling access to premises or for managing private spaces in the workplace are not allowed to continue after the crisis, as this could create distrust and lead to a state of emergency that would become or be perceived as permanent.

The danger would in effect be the gradual **trivialization** of the use of tracing technologies and becoming **accustomed** to the practice of monitoring citizens and employees. The mindsets we have reviewed make us aware of the impact they can have on our perceptions and decisions and taking those into account can inform both governments and companies on the choice of appropriate technologies and governance methods.

Thinking of the current situation from the mindset of care, which seems to us to be the most appropriate for the public health situation we are in and for the broader societal challenges it raises, implies that crisis exit strategies should be based on principles of inclusive governance, dialogue, solidarity and equity, accountability and trust. In contrast to the idea that the responsibility to defend ourselves lies with government and that the danger is external (even though we may all be carriers of the virus), such a mindset requires us to continuously strive for a fair compromise between the need for individual freedom of choice (autonomy) and the responsibility to care for each other (health), while giving absolute priority to protecting the most vulnerable populations.

CHAPTER 2

UNDERSTANDING THE CHARACTERISTICS OF TECHNOLOGIES

Selecting a technology to resolve a problem is **never neutral**. Not because of the technology itself, but rather because of the conditions of acceptability and governance required for their effective and appropriate use.

With this in mind, **four purposes** of the IT-based approaches to exiting the crisis and reopening the economy were analyzed: (1) **tracking** individuals carrying the virus, (2) **studying** community-wide **behaviours**, (3) **monitoring compliance** with health measures, and (4) **controlling access** to private spaces.

For each of these areas, the **choice of IT architectures and solution governance methods are closely linked**, so decisions by public or private decision-makers must be based on this inseparable whole.

Some dozen tracing applications developed throughout the world were analyzed and discussed. The **risks** that these technologies could present were also raised, as well as the **options available to mitigate them**. These considerations may assist decision-makers in the **trade-offs** to be made in a highly complex context dictated by emergency.

The important challenges identified in this work include the **type and accuracy of the data** collected (**GPS** location data vs. **Bluetooth** proximity data), application **interoperability** both nationally and internationally, and **interdependence** with third party systems.

There has been intense, and often heated, debate around a centralized versus a decentralized system. Our analysis shows that this apparent dichotomy must be nuanced: many responses are hybrid, integrating both centralized and decentralized components. However, this is a particularly **impactful** decision, both in terms of IT security measures and respect for individual rights, as well as in terms of governance arrangements.

According to a number of recent studies and publications, over 40 tracking applications have been developed or deployed in more than 20 countries. Alternative measures for digitally tracking individuals (wristbands, cameras) and technologies for monitoring (movements or body temperature) the public were in use in some 30 countries. These developments are either the result of private initiatives, led by independent non-profit organizations, or initiatives actively supported by public authorities. All in all, techniques for managing and controlling the health crisis using digital tools are currently being developed in very different ways in well over 50 countries. This report presents a typology of the IT-based technological approaches to a health crisis exit strategy. It sets out their main technical characteristics in order to illustrate their influence on governance methods and to alert public and private decision-makers to the importance of the IT-based option and the impact it can have on society, their public administration or their businesses and how they are organized.

TYPOLOGY OF TECHNOLOGICAL DEVICES FOR COMBATING COVID-19

International attention and debate has so far focused particularly on the **tracking applications** studied by governments. However, it is important to bear in mind all the technologies that can be used in the context of a health crisis exit strategy. In particular, major challenges will arise **for businesses** that choose to deploy tools for monitoring employee health, whether by collecting **health data**, processing **movement data** or encouraging (or even requiring) the use of a smart device.

Given the proliferation of these tools, multiple classifications are possible. We have opted for a typology which breaks down the IT-based measures according to the four main approaches:

1. TRACKING INDIVIDUALS CARRYING THE VIRUS
2. STUDYING COMMUNITY-WIDE BEHAVIOURS
3. MONITORING COMPLIANCE WITH HEALTH MEASURES
4. CONTROLLING ACCESS TO PRIVATE SPACES

The diagram below shows the different aims associated with each of these approaches as well as the techniques that can be used.

Typology	Tracking individuals carrying the virus	Study of community-wide behaviours	Monitoring compliance with health measures	Controlling access to private spaces
Example	Contact tracing	Mapping the public's movements	Smart electronic symptom detection bracelet	Controlling access to workplaces and stores
Purpose	· Automatically notify individuals who have met a person who has tested positive to allow those at risk to manage their isolation · Identify the main vectors of infection in order to take appropriate measures · Notify property owners and employers that individuals testing positive have been on the premises, and manage cases requiring building or workplace closures · Improve peoples' understanding of risk factors and probabilities of contagion	· Provide real-time information on virus spread · Anticipate population trends to adjust resource requirements (e.g., within hospitals) · Measure the effectiveness of the public policy measures implemented · Monitor unusual concentrations of people in public spaces for effective response · Improve peoples' understanding of risk factors and probabilities of contagion	· Monitor compliance with containment measures by affected individuals · Measure effectiveness of compliance rules · Restrict unauthorized travel and movement · Accurately identify symptoms and offer effective detection solutions · Provide medical assistance to individuals	· Assist employers in their duty to ensure employee safety · Enable reopening of businesses · Prevent the virus from entering the workplace or supply chain (within businesses, their business partners and customers) · Regulate, authorize or prohibit access to a store, business, private space, etc. · Assess personal risk for employer management of workplace exclusion cases
Technique used	· Bluetooth · GPS · Ultrasound · Phone cell tracing · Video surveillance	· Phone cell tracing · GPS · Bank cards · Social media	· Sensors/IoT · GPS · QR codes · Drones · AI systems	· Thermal cameras · Facial recognition · Chatbots · Blockchain use · Smart devices · AI systems

There are many examples for each of these four categories. This list is not intended as comprehensive, but rather to illustrate their diversity and outline their main characteristics.

1 TRACKING INDIVIDUALS CARRYING THE VIRUS

For the purposes of this report, we have, in particular, extensively studied a number of initiatives in the first category, namely tracking. In particular the **DP-3T, TraceTogether, COVI App, ROBERT, Apple/Google API, Aarogya Setu, COALITION**, or **NHSx** initiatives, based on publicly available online documentation. A comparative table of these projects is appended to this report (see Appendix 3), as well as more specific analyses (see Appendix 4). The vast majority of these initiatives collect personal data through the use of Bluetooth technology (some also use GPS data), use technical encryption measures (mostly for data "at rest", sometimes also for data "in transit", i.e., while it is being transmitted) and pseudonymization of data.

It should be noted that many publications refer to the anonymous nature of the data collected, which must be largely qualified. On the one hand, because the definition of **personal data** varies from one continent to another (see, for example, the difference between *personal data* and *personally identifiable information* — PII). On the other hand, because the standards for recognizing the anonymous character of a data item are not uniform from one country to another, some refer to it as **anonymized** data, which would imply that it is irreversibly impossible to re-identify an individual, while most of the time it is simply **pseudonymized** data, i.e., data for which the identification of the data subject remains technically possible. Decision-makers must therefore be aware that in deploying these solutions, the data processed will most certainly be in personal and non-anonymized form. Finally, some data may not at first glance appear **sensitive**. This is so for notifications sent to individuals considered infected. Nevertheless, it should be noted that merely notifying an individual could potentially in itself be considered as health data (see in particular Appendix 4).

Furthermore, several distinctions must be noted. Firstly, the difference between a **protocol** and an **application**. A protocol is a set of rules that govern the operation of a tool (be it an application, a smart device, etc.). Thus, a protocol defines the rules and procedures allowing IT processes to exchange data. An application, on the other hand, is software used to perform a task. An app runs on an operating system (e.g., the Operating System (OS) of a computer or smartphone) and follows the rules of several protocols. For example, the StopCovid application is based on the ROBERT protocol. But StopCovid could also have opted to use the DP-3T protocol. Conversely, the BlueTrace protocol was used in the TraceTogether app by Singapore as well as by the Australian government, which developed its own COVIDSafe app, based on feedback from the Singaporean app.

Without going into overly technical considerations, a distinction should also be made between applications and APIs (Application Programming Interfaces), which are programming interfaces allowing an IT entity to interact with third-party systems. This raises important issues of dependency. In fact, **application interdependence** with third-party systems creates potential exposure to IT access to the data stored in an application. Equally sensitive is the issue of interoperability. For example, Apple and Google jointly offer an API which is only compatible with applications that run on decentralized systems. This API enables tracking applications to be used on smartphones with Android (Google) and iOS (Apple) operating systems, while maintaining user privacy. The issue of system interoperability is fundamental and has already given rise to much controversy in some countries, such as France (where the ROBERT protocol is considered centralized and is not compatible with the Apple/Google API). The application developed by NHSx — which has long wavered between a centralized and decentralized approach — could encounter similar problems.

Another important distinction must be made between a **technology** and **how it is used**. Debates about whether these devices should be deployed on a mandatory or voluntary basis revolve around the context, both legislative and political, in which a technology is deployed, but not the technology itself. Thus, although a protocol or an application is "mandatory" per se, its use may or may not be mandatory. That depends on the **context** in which it is implemented. Thus, the same application may be mandatory in one country and optional in another. In India, the Aarogya Setu app is one of the few

initiatives to be made mandatory, under threat of criminal prosecution (the government later changed its position).

In addition, when a tool is intended for use by governments and businesses around the world, there is an inherent risk for citizens and employees

residing in countries that do not have laws and regulations governing data protection, safety in the workplace, or anti-discrimination. For example, some countries such as Australia have already amended their national privacy legislation to introduce specific provisions for the national privacy authority — the Office of the Australian Information Commissioner (OAIC) — to exercise oversight over application data; establishing a data deletion process at the end of the pandemic; and requiring the Minister for Health and the OAIC to submit enforcement reports. Other countries currently do not have general application legislation that would apply to the collection, use and disclosure of personal information through contact tracing applications; and still others do not have a body of law ensuring that fundamental rights are upheld.

We thus understand the importance of using, as far as possible, IT-based tools that by default and by design safeguard individual freedoms and fundamental rights. On the other hand, we can also appreciate that a device's effectiveness or technical features may sometimes be inadequate, particularly when their use is not governed by sufficiently robust legislative or regulatory protection requirements.

We should not underestimate the cultural aspects of our relationship to technology. As such, Singapore is a socially cohesive country, that is, a society with a high degree of trust in government. As a result, TraceTogether and other applications using the BlueTrace protocol could have difficulty achieving the general acceptance necessary to be effective in jurisdictions that do not share those traits. For such countries, deployment of that type of application would certainly entail mandatory regulations in order to achieve the expected societal benefits.

Finally, the issue of whether a SARS-COV-2 diagnosis is **accurate** and **verifiable**, scarcely discussed in the literature, is an important selection criterion. The ten or so initiatives studied break down into two types of approaches in equal proportion: self-diagnosis versus verified diagnosis. For example, the TraceTogether initiative operates on the basis of verified diagnosis, involving a screening verification procedure by government agents responsible for tracing contacts, which provides more accurate data. Conversely, self-diagnosis (as with NHSx or COALITION) only takes symptoms into account, without a medical diagnosis, which increases the likelihood of false positives. The use of a self-diagnosis based application also depends on the relative ease or difficulty of access to screening tests as a condition for obtaining medical confirmation of infection. In any event, there is a legitimate concern that an IT-based device could provide a digital **risk score**, which might lead to a heightened sense of panic in a user with a high score. In this respect, the chosen technology developed for COVI-App is interesting. In fact, the application is configured to provide information and **recommendations**, rather than a raw, uninterpretable score. Instead of providing a binary (yes/no) assessment of whether an individual has been in contact with another individual diagnosed with COVID-19, the COVI-App machine learning solution developed by the MILA calculates the overall probability of user exposure to COVID-19 (the risk score), based on demographic, health and behavioural information provided by the user, official diagnoses, if available, and the risk of other network users. This choice of technology aims to empower users by enabling them to adopt appropriate behaviour based on their level of risk.

2 STUDYING COMMUNITY-WIDE BEHAVIOURS

The purpose of the **second category** of IT-based devices is to analyze behaviour, not on an individual level, as do tracing applications, but **community-wide**. This does not involve processing personal data, but **aggregated statistics**. This practice is found on several continents. In the United States, for example, researchers have been able to use location data from Facebook users who share their location history to develop maps measuring physical distance. In China, Baidu used its mapping service to model areas of contagion in real time. In Finland, telecom operator Telia shares anonymized cellular location data with the government to enable monitoring of population movements and identify at risk areas.

In some cases, these practices involve the use of **data from telephone cells**, which transmit information from mobile devices without requiring user activation. In other cases, processing **GPS data** from mobile apps requires user activation. The data are aggregated and used to generate check-in

reports. On a more trail-based level, **the credit card system** allows transaction locations to be traced and, by aggregating the data, provides a map of user movements.

3 MONITORING COMPLIANCE WITH HEALTH MEASURES

The **third category** of technologies relates to smart devices that allow for monitoring individuals' status and their compliance with **containment measures**. Once again, while not claiming to provide a comprehensive analysis, we cite a few to illustrate the diversity of approaches. In Australia, some quarantined people may be monitored via a camera installed in their home or may be required to wear a smart bracelet. In Poland, individuals in confinement are asked to download an application that prompts them to take geo-localized selfies. Agents then verify that these people are at home by sending messages and analyzing location data. In Hong Kong, persons in confinement are required to wear a smart bracelet which, combined with an app, allows the authorities to monitor quarantine compliance. In Taiwan, persons in home confinement receive calls from government agents twice a day and risk publication of their identities and fines of €30,000 if they are absent. Russia's government uses cameras combined with a facial recognition system and phone location data to monitor individuals under quarantine.

This report looked at an innovative approach launched in Germany by the **Robert Koch Institut** (RKI). The German govenment's federal public health agency released a data "donation" application called Corona-Datenspende. Designed by RKI, the application enables users to donate health data to the agency from their smart clothes, wristbands and wellness apps. The goal is to derive information from these data on the spread of COVID-19 at the national and regional levels. Our report looked more specifically at this initiative, which has the unique feature of improving the ability to predict the spread of COVID-19 using nationally based on non-specific health data (such as pulse rates) and thereby accelerate and target future containment measures in identified high-risk areas. That being said, the project is designed to serve public health rather than to give the donor an indication of whether or not they are infected. Given that testing capacity is limited and that many COVID-19 infections show only very mild symptoms (so infected individuals will probably never seek testing themselves, but may nonetheless transmit the virus to others who may develop more severe symptoms), the RKI aims to improve the rate for estimating the number of possible undetected COVID-19 infections.

4 CONTROLLING ACCESS TO PRIVATE SPACES

Lastly, the **fourth category** includes applications that can be deployed within businesses and **private spaces**. While attention thus far has been focused primarily on applications that can be implemented by governments and the issues surrounding tracking, initiatives by private businesses should be carefully studied. They will most certainly take a greater place in the future and require serious consideration as they are impacting and will continue to impact our lives and actions. In any event, employees should not be forced to adopt the tool, but rather be fully involved in it. Voluntary employee buy-in for the tool will be all the easier.

In a work environment, the "voluntary" element around using the tool may need to be clarified. Like many other tools used in a work environment, their use may become a mandatory condition of employment, as long as requiring employees to use the tools does not infringe on applicable law.

However, the fact that employers may have the legal right to impose the use of certain technologies on employees in the workplace does not mean that they are "obliged" to impose new technologies with monitoring capabilities without first giving the affected employees the opportunity to participate, at least to some extent, in the decision-making process related to the selection and deployment of these tools, as part of an inclusive governance process, as discussed in more detail in Chapter 3.

The purpose of these devices is to measure employees' state of health to determine whether or not they can enter the workplace. For example, British telecom operator Vodafone and remote surveillance company Digital Barriers have developed a thermal smart camera to detect any employee with a fever.

Québec-based OPTEL has launched a mobile application designed to make premises more secure. The application asks employees to answer questions about their health, through a chatbot, and to enter their workplace if the risk is considered low. In France, Crédit Agricole and Onepoint worked together to develop the “Copass” (digital badge) application to manage the reopening of businesses. By answering a health questionnaire, employees are given a COVID-19 “sensitivity level’ to help businesses establish organizational protocols (teleworking, staggered working hours, etc.).

Software developer ONHYS simulates the flow of visitors, users, patients or employees within an establishment. The software tests different layout configurations to identify the solution that best reduces the risk to people. To ensure physical distance in the workplace, Landing AI has developed a detection tool based on artificial intelligence, which models the distance between people based on real-time video streams. This system has already been deployed in factory and industrial site security cameras.

In particular, this report looked at two use cases. The first, developed by Canadian business TerraHub, is an example of an "immunity passport" based on blockchain technology, allowing employees to voluntarily share health data, while controlling access to it. TerraHub decided to adapt its Credential Link solution to implement functionalities for accelerating and facilitating the return of employees after the confinement period. Based on the Hyperledger Fabric blockchain protocol, Credential Link allows employees to self-declare their state of health on a daily basis or to download additional proof of their ability to return to work safely. An algorithm that produces a health summary is sent to their employer each day to assist the employer in implementing security measures.

The second use case studied is a connected object developed by **Estimote** in Poland. Called Proof of Health, its aim is to enable employers to anticipate virus spread among employees. The device has a button employees can use to alert management of an event (symptom, infection). The device includes a GPS system, as well as Bluetooth-powered proximity sensors and ultra-wideband radio connectivity. The solution's effectiveness depends on reporting by the infected employee and the onset of symptoms. Due to its high-tech features, this type of application presents significant ethical risks of tracing each employee's movements within a building, measuring time at a workstation as well as break times, or even the frequency of interactions between employees (and perhaps even outside the workplace or outside working hours). No information regarding security or data stored on the device and server seems to be available for the Estimote device.

In this context, *The Coronavirus (Safeguards) Bill 2020* in the UK is interesting to consider, as it attempts to provide appropriate safeguards for the symptom tracking and contact tracing applications currently being deployed in the UK, and provides for minimum safeguards that will be required if we move to deployment of "immunity certificates" (commonly known as passports) in the near future. It does not specify any particular IT-based approach for creating applications and does not attempt to replicate the GDPR and ePrivacy guidelines. Rather, it suggests some basic safeguards that need to be added to what these rules already provide.

More specifically, the bill states that:

(a) No one shall be penalized for not having a phone (or other device), leaving house without a phone, failing to charge phone, etc.;

(b) No one is compelled to install a symptom and contact tracing app, or to share messages of their status on such an app (e.g., with an employer, insurer or university);

(c) Personal data collected by an app, or contained in an immunity certificate, shall not be shared beyond the NHS and coronavirus researchers unless securely anonymized;

(d) What is true, secure, verifiable, anonymization needs to be certified by a stringent Code of Conduct;

(e) Personal data collected by apps or immunity certificate must be deleted or anonymized as soon as possible, or at latest immediately after the emergency period has expired;

(f) "Immunity passports" must not become novel and uncontrolled internal passports, nor used by either state or private sector to discriminate in ways not necessary or proportionate to the legitimate social goal of controlling COVID-19.

TECHNICAL CHARACTERISTICS INFLUENCE MODES OF GOVERNANCE

Analysis of the measures developed to manage the health crisis shows that the choice of IT architecture has a direct influence on how it is governed: the type of technologies used, the methods of data storage, the choice of a centralized or decentralized structure all have an impact on the entire initiative and on its social acceptability. Professor Lawrence Lessig's adage "code is law" is more topical than ever. Certain technical characteristics must therefore be known to decision-makers who have to evaluate and choose an IT-based approach, in the public sector or in companies.

Currently, contact tracing applications have been the subject of the most intense public debates. Information on their technical characteristics is the

most readily available, which is sometimes accessible in the form of open source documentation. We have therefore decided to use these applications as a case in point to highlight the governance issues they raise and illustrate the challenges raised by the deployment of IT-based devices. This analysis can be used to study other types of technologies, such as those mentioned in categories 2, 3 and 4 of our typology.

AVOIDING TWO TRAPS: REDUCTIONISM AND SOLUTIONISM

Before choosing an IT-based response, decision makers must bear in mind two important potential biases: reductionism and its corollary, solutionism. **Reductionism** consists in "reducing" reality and all phenomena to mathematical equations that are used to reach a decision. This trend is considerably reinforced by big data. Algorithmic processing has its advantages, but also carries significant risk of taking the measure (i.e., the observed correlation) to be the cause of the phenomenon (i.e., the causality of that measure). The actions and notifications associated with tracking applications (i.e., warning messages sent to users) are not explainable to users, as they do not obtain any information about the location or exact time of contact. Users have to trust the application without being able to obtain other information about the "real" risks, for example the percentage of associated risk of infection, which would be a function of contact time, proximity, and other possible factors.

The study carried out on tracking applications highlights the danger of relying unthinkingly and uncritically on a measure that can lead to automation bias (unconditional reliance on the results obtained by the application) or to ostracizing others. This puts these devices on the brink of becoming proxies for social interactions, because adopting them could condition human relationships positively (I tested negative, so I can interact) or negatively (I'm at risk so I'm an outcast). This artificial alteration of social relations therefore has the potential to strengthen or, on the contrary, weaken peoples' confidence not only in the people around them but also in government, institutions and public authorities.

Without being overly simplistic in criticizing technology, we must also guard against a tendency towards **techno-solutionism**, which aims, by solely technical means, to resolve problems that are essentially social and political, such as those posed by a pandemic crisis situation, which is a public health issue involving national and international solidarity. **In this way, technology can become an alibi for decision-makers to excuse the lack of other initiatives.** A related issue is the IT imperative: that is, the moral obligation to use an IT-based "solution" because it exists. However, just because an IT-based tool is available does it not necessarily mean it is the most suitable response (i.e., the most effective, efficient, socially acceptable or ethically responsible) to the problem in question.

Thus, operational efficiency (What is the detection quality? What is the rate of false positives? etc.) and ethical acceptability of a digital application for combating COVID-19 can never be analyzed in isolation from other health measures or social processes. Experience shows that the countries which pioneered the use of digital tools for combating COVID-19, such as China, Taiwan and South Korea, derive effectiveness from using technology only by carefully fitting it into a much broader global and multidimensional crisis governance policy. Social and political participation by communities and intermediary bodies, intervening between the individual and the government, makes it possible to continuously monitor the effectiveness of digital tools and how they are adapted to human needs in fighting the pandemic.

CHOOSING TECHNOLOGIES AND THE DATA COLLECTED

A first aspect concerns the type of technology used and the type of data it can collect. With regard to applications for monitoring virus carriers, it should be noted that they can identify people who have been in close proximity to an individual reporting symptoms, but they cannot identify possible contamination by an asymptomatic patient or by a person who does not declare his or her condition to the medical authority. Technology is part of the solution, but its effectiveness depends on human factors.

The type of data collected by tracking applications can be either location or proximity data. Location data allow the position of an individual to be tracked and can be gathered by GPS technologies; proximity data provide information on the interactions between people (contact or passing nearby...) that could be occasions for spreading the virus. They are accessible via Bluetooth.

While the chips in smartphones communicating with the GPS satellite network give a position to the nearest metre, their accuracy is impaired in urban environments, especially if the user is in a large building. This makes it difficult to use them in situations that could be hotbeds of transmission. **Bluetooth**, on the other hand, locates a device in relation to other smart devices nearby. It works well inside buildings. However, the technology is not designed to gauge distances. The signal range depends on the quality of the device, its position (hand-held, in a pocket or luggage) and the battery charge status. Moreover, the technology cannot establish with certainty that there has been contact: the signal transmits easily through a window (train, car at a stop sign, building...) and cannot detect spread by indirect contact, such as touching an infected object, or by suspended droplets in the airflow of an air-conditioning system.

TECHNICAL RISKS AND BLUETOOTH COMPUTER SECURITY ISSUES

Of the ten or so initiatives reviewed as part of this project, the majority are based on Bluetooth technology, or **beacons**. Devices with the application signal each other by sending a short (16 byte) signal, allowing any device to detect another device signalling nearby.

Thus, it is impractical for a device to send messages that are to be understood only by a limited number of authorized devices, while the algorithm for handling these messages is public. Under these conditions, it is easy for anyone with a modicum of IT skills to intercept Bluetooth signals and even spread malicious information using their own software, or a modified version of the original software. For example, the range of a Bluetooth signal varies depending on the equipment used, with a dedicated antenna being able to pick up the signal up to several hundred metres away in open terrain. However, it is impossible to limit a Bluetooth signal to a maximum of five meters on a smartphone, and the same is true for reception.

Knowing this, we can see there is a wide array of more or less damaging attacks that can be carried out against tracking devices. A first possible scenario for attack could be to send a mass of wrong information to corrupt the application data and render it useless. An attacker with the technical capabilities to intercept and engage with the large-scale solution could also link the data collected with other information (geolocation, time indicator, photo/video capture), to re-identify users who have tested positive for COVID-19. It is perfectly feasible to then extrapolate this information in order to link it to previously targeted groups of individuals or communities.

These attacks pose a risk to some of the main requirements for tracking applications: data accuracy, medical confidentiality, anonymity, meeting privacy (locations, dates, identities). Accordingly, the DP-3T project has been particularly vigilant with regard to all of these risks and constantly improves its protocol in order to mitigate or even prevent them.

Servers for centralized solutions (for example, the ROBERT protocol project), are able to associate these few bytes with a device identifier and a specific date. Contact graph anonymity and privacy are more vulnerable in this case. For the DP-3T protocol's decentralized solution, the few bytes transmitted by a device simply represent a fleeting random value associated with raw date data. Only the transmitting device would be able to identify its information as originating from itself. Consequently, in this solution, compromising data privacy is more complicated. By bearing in mind some of these technical elements, decision-makers will be able to assess whether or not the technical **risks** and IT security issues they present leave **a trail or not**, in order to assist in selecting the IT-based response to be deployed.

CENTRALIZATION VS. DECENTRALIZATION: AN IMPACTFUL CHOICE

The choice of a centralized or decentralized system is particularly impactful. Centralization and decentralization are often explained in IT as a sharp dichotomy. As we shall see, the reality is more subtle and complex.

Both systems are viable technically speaking and have their pros and cons in terms of security and infrastructure. The main difference is not technical but lies in the concepts we want to instill in those systems with respect to our societies, rights and duties, laws, and ethics. Accountability and privacy are the first of those concepts.

Decentralized systems (more or less like DP-3T or COALITION) by definition spread the roles to different actors who take part in the system. Accountability in a decentralized context becomes a chain of responsibility: a decentralized system works if the chain of responsibility is ensured by enough fair actors in the system (not necessarily all of them). Those systems are inspired by the more general concept of "decentralization" which links to the concepts of participation in decision-making, local representation, democracy, equality and liberty. Yet, due to the increased number of responsible actors in the system, it has a cost in terms of upstream specifications, downstream rigidity and more complex security processes and systems.

It also poses the issue of the malicious user who sends wrong or even crafted data to spoil the whole system (that can be mitigated by mechanisms of authorization with more or less centralized certification authorities). It also raises the issue of global governance of the system with respect to laws in countries and across borders.

A centralized system (more or less like ROBERT) is aimed at gathering the responsibility in one central entity (the central server) which ensures the whole system is consistent and coherent. This kind of system works perfectly when a single entity is able and is required to endorse the whole responsibility (especially in the context of organizations such as states or cross-border organizations such as the EU). The central entity manages everything much more easily: the level of authentication and authorization of users, the data life-cycle (security, authentication, certification) and the evolution of the infrastructure. But this naturally implies that this central entity is fully trusted by users and does not misuse the data (A "trusted third party").

Risks of using such centralized system include the following:

- **Single point of attack:** Any breach in a server would endanger the whole federated system and all users of affected applications. Intrusion into the server could result in the identification of users.

- **Linkability of users:** With a centralized system, the server is able to learn and potentially piece together information about specific users. The server could infer that two infected users were in contact at some point in time based on timestamps, allowing the server to build a partial social graph that reflects these encounters. Furthermore, the server could identify anonymous uploaders with co-locations by performing a frequency analysis on the uploads and cross referencing with who performed the uploads. In addition, the server could identify anonymous uploaders with causality, as causality is preserved in the uploads. Thus, the server can reconstruct a pseudonymous graph using time causality.

- **Tracing of users:** The centralized server creates ephemeral identifiers and can, at any point, link the past and future ephemeral identifiers of any user, infected or not, by decrypting back to their permanent identifier. In combination with other data sets, such as CCTVs, the server can therefore track all individuals, infected or not. Given a target ephemeral ID, such as one collected by law enforcement from a suspect, it is possible to tag and classify individuals that third parties can recognize without access to the centralized server or database. For instance, ROBERT's ephemeral IDs are not authenticated, and the server does not provide any proof that they are an encryption of the ID, or that the correct key was used. This capability could allow law enforcement, or other actors, without any access to the backend database, to track the movements of specific users and communities by assigning them distinguishable identifiers and recognizing their tagged Bluetooth emissions. This could enable long-term tracking of individuals or communities (as one could assign specific identifiers to target groups of people) by third parties.

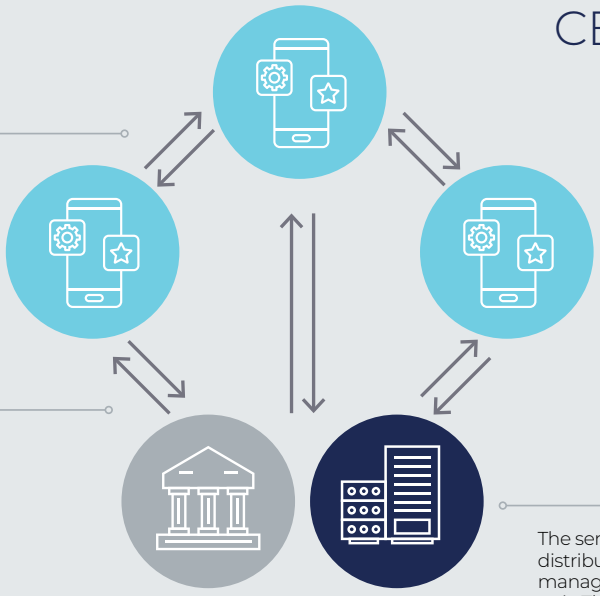
- **NB.** These are hypothetical attacks which represent a potential risk and will depend on the mitigation means implemented in the solution when in production. There are ways to reduce the risk as the DP-3T specs show it.

Both centralized and decentralized systems can scale their boundaries to mitigate their respective drawbacks while also paving the way for new kinds of attacks:

- Example 1: The ROBERT protocol delegates data collection and obfuscation to users but keys are generated by the central server. It then opens the door to possible attacks by malicious users injecting bad data. It is unclear, in the related StopCovid application, whether a validation step with an authority is to be implemented, thanks to the QR Code between the health authority and the app.

CENTRALIZED SYSTEM

Only scrambled information (obfuscation) is exchanged between physically close devices. Private information never leaves the device in these

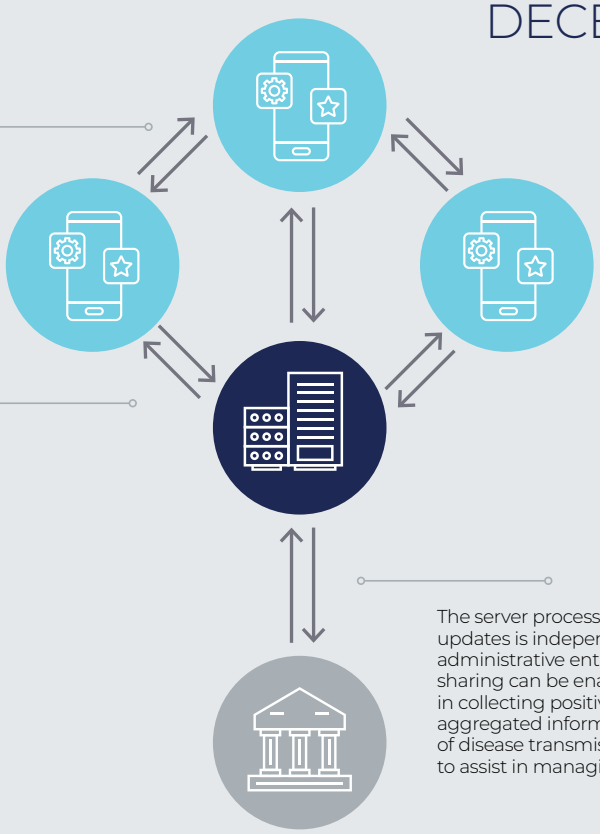


The updated information is transmitted to a central server that processes and distributes the updates throughout the users' network. In contrast to the decentralized model, here the exchanges contain key contact tracing information. Information security is ensured through several encryption and anonymization protocols.

The server processing and distributing the updates is managed by an administrative unit. This leverages the maximum amount of information from contact tracing for the benefit of a centralized health crisis management strategy.

DECENTRALIZED SYSTEM

Only scrambled information (obfuscation) is exchanged between physically close devices. Private information never leaves the device.



The updated information is transmitted to a central server that processes and distributes the updates throughout the users' network. The shared information is not useful in itself. Only the application of each device can transform these updates into useful information for users.

The server processing and distributing updates is independent of the administrative entities, but update sharing can be enabled, for example, in collecting positive diagnoses. Some aggregated information on the evolution of disease transmission can be produced to assist in managing the health crisis.

- Example 2: Decentralized systems need to authenticate and certify users to mitigate the issue of malicious users. But an authentication authority is a more centralized system so it again raises the issue of trust.

Thus, the **apparent dichotomy** between centralization and decentralization is actually more subtle than this, as some elements of a solution can be decentralized while others cannot. So much so that most IT-based responses appear in reality **hybrid**, through a choice of both centralized and decentralized components.

Several consequences flow from this, as outlined in the table below. For example systems like DP-3T/Coalition are partially decentralized: they decentralize the collection, exchange and checking of contact data on the client-side: people are responsible for their own data. But the storage of infected users' data is still centralized in a central server. We could imagine pushing decentralization further by decentralizing the storage itself.

Comparison based only on (de)centralization aspects and high-level features for which there are remarkable differences.

Categories	ROBERT	DP-3T	Coalition	Google/Apple	MILA
Bluetooth Tracing	Yes	Yes	Yes	Yes	Yes
GPS Tracing	No	No	Yes (for coarse localization)	No	Yes
Contact Data Collection	Decentralized	Decentralized	Decentralized	Decentralized	Decentralized
Contact Data Ciphering	Decentralized	Decentralized	Decentralized	Decentralized	Decentralized
Contact Secret Keys Generation	Centralized	Decentralized	Decentralized	Decentralized	Decentralized
Contact Data Storage	Centralized	Centralized	Centralized	N/A	Centralized
Risk of infection Evaluation	Centralized	Decentralized	Decentralized	Decentralized	Decentralized
Contact Data exchanged when declared positive	Send Others Contact Keys	Send Others Contact Keys	Send Others Contact Keys	Send Others Contact Keys	Send Others Contact Keys Send Obfuscated location
Contact Data exchanged when checking risk of infection	Send Others Contact Keys	Download Infected Users Contact keys	Download Infected Users Contact keys	N/A	Download Infected Users Contact keys
Private user data collection	No	No	Coarse location	No	Yes
Future Predictive System	No	No	No	No	Yes
Can be cross-border System	Yes	Yes	Yes	N/A	No
Can be used for more than contact tracing	No	No	No	No	Yes
Requires human authentication authority when declared positive	Possibly	Possibly	No	N/A	Yes
Relative Server Infrastructure Complexity (1: basic to 5: complex)	2	3	3	N/A	5
Open source	Partially opensourced (protocol + data model)	Yes (mobile and server SDK)	Yes (mobile library)	TBD	TBD
Organization	Governmental	Non-profit	Non-profit	TBD	Non-profit

s. o. : sans objet

RECOMMENDATIONS

Effective technologies can be used without sacrificing our individual freedoms and fundamental rights. An informed choice of technologies requires knowledge of their underlying technical characteristics.

And understanding of the technical aspects must be shared — through an appropriate educational initiative — across an entire organization or population in order to foster buy-in. For example, to limit any digital divide, inclusiveness and information are required (Do your employees know what Bluetooth is, how a blockchain works, where data is stored? Do you intend to disclose your technology's potential percentage of false positives, etc.?) Both governments and businesses must take care not to compound the consequences of unequal access to technology or risk penalizing those who are already largely excluded from the digital world. Moreover, the information provided to users must make it very clear that no application can be considered as a medical device, despite the notifications and guidelines, and that it is not a substitute for a screening test.

Comparisons drawn from benchmarking tracing applications help to illustrate the questions that need to be asked. These issues also apply to the deployment of other types of technologies (connected devices, thermal cameras, AI systems, blockchains, etc.), with the benchmarking process adapted to the particular features of each planned project.

Given the circumstances, decision-makers must develop a critical view with regard to selecting IT-based solutions. For example, where the code for a proposed tool has not been checked by independent third parties, there is no guarantee it will process the data as stated by the project promoter. For that reason, we recommend providing for an independent control body, which seems particularly appropriate as part of a governance system, and third-party auditability, which is particularly suited for businesses. A further recommendation in this respect is to oblige providers to conduct separate and publicly accessible impact measures (such as the one set out in **Appendix 2**).

Technical measures alone will certainly not suffice to guarantee that individuals are protected. Governments must bear in mind the importance of the **legislative, social and political context** in which such solutions could be deployed. Accordingly, it would be necessary to enact appropriate legal and regulatory provisions to safeguard individual freedoms and fundamental rights and to avoid discriminating against or stigmatizing certain groups.

Finally, beyond or additionally to any immediate objectives for a technology's usefulness, decision-makers would have to factor **ecological transition needs** into the preferred IT-based solution. The health crisis must not overshadow the climate crisis facing humanity and every human being.

CHAPTER 3

DEFINING A GOVERNANCE MODEL

By basing our understanding of the situation on the appropriate mindset and armed with detailed knowledge of the various technologies available, we can build an IT-based strategy to combat the pandemic, restart economic activity and, more generally, operate in the post-crisis landscape.

To make the most appropriate choices and ensure the project is positively received, **the key success factor in our opinion is governance**. The method detailed in this chapter could inspire decision-makers in developing their strategy and particularly in deciding how IT-based tools are selected, deployed and managed.

This method is based on six principles, **which guide the entire approach, and on a participatory mode of governance**. The current crisis context calls for innovative solutions and real social acceptance, both of which will be helped by the inclusion of all stakeholders from the outset of the decision-making process. The presence of **technical, legal and ethical experts** within the governing body also seems crucial to us.

During the methodological stage of validating the choice of a technology, these six principles will take the form of **concrete criteria put together in an evaluation matrix**. This document, compiled by the project's participatory governance body, will address all aspects of the technology under review and provide a basis for discussion in the decision-making process. It can be used as a guideline throughout a project managed in agile mode, to ensure that the measures taken are consistent with changes in the health and economic situation.

This method can be used by any type of institution. **Specific recommendations for its deployment in businesses** are provided in the framed text at the end of this section.

Our report shows how essential it is to determine the appropriate framework for dealing with this protean crisis, particularly in terms of health and socio-economic issues (see Chapter 1). Knowledge of the characteristics of technologies is equally fundamental to understanding their influence on our individual and collective freedoms and how our societies are run (see Chapter 2). We need to determine how a governance model can be defined for the technological solutions under consideration. Indeed, SARS-COV2 is having and will continue to have an unprecedented impact on the functioning of our organizations, particularly businesses. Accordingly, governance should be based on key principles. In this last section of the report, we propose a two-tiered analysis: first, we will identify ethical values and legal standards and secondly, they will be linked to different criteria in a multi-factor impact matrix. With this impact matrix – which is intended to be a sound governance tool for the responsible deployment of COVI technologies and whose instructions for use are detailed below – we can go beyond the simple assessment of data protection or the simplistic conflict between individual privacy and public security and propose a concrete method for selecting and deploying crisis exit solutions. In this third chapter, we address the need for inclusive and participatory governance to avoid any disruptions to social bonds, and more specifically how solutions can be implemented in businesses.

METHODOLOGY FOR SELECTING, DEPLOYING AND GOVERNING AN IT-BASED HEALTH CRISIS MANAGEMENT STRATEGY

The specific nature of pandemic risk implies that restarting economic and social activity requires that organizations develop a **type of herd immunity and resilience**. This approach calls for active buy-in and responsibility on the part of everyone within an ethical culture of technology use. It requires a participatory approach that can put IT-based choices in context and build in the diversity of real-life situations experienced by the different stakeholders and the ethical issues they face.

Moreover, the inextricable link between technical, legal and ethical aspects forces us to address the issue of deploying IT-based tools **systemically**. We therefore propose a **multi-factor matrix method** implemented by a **multidisciplinary** team.

The analysis begins by studying **the objectives** that an IT-based tool must achieve, through its purpose, the context in which it is developed or the ecosystem in which it is integrated: its effectiveness must be assessed in the light of the entire strategy it is deployed within.

Next, we analyze the **technical characteristics** of the devices under consideration. For example, an application using a centralized or decentralized protocol implies far-reaching governance choices. Similarly, the issues of interdependence and interoperability with other external technologies can be crucial.

In addition, challenges related to **social acceptability** need to be addressed. The risks of fraudulent or wrongful use of the solution must be considered, as well as other social risks, such as the widening of the digital divide or forms of discrimination.

The question of temporality is also key: an IT-based solution needed to exit the crisis may end up being disproportionate. The criteria that characterize a “crisis situation” within an organization should be determined. Should the solution be used as long as epidemic outbreaks are identified around the world, or if the disease takes the form of a seasonal epidemic? Is it necessary to adopt a logic of preventing of a new epidemic?

In practical terms, to implement the method advocated here, **the first step is to set up an appropriate governance body**, involving representatives of all stakeholders with technical, legal and ethical expertise. This body will guide the project end to end.

Firstly, we recommend that such a group familiarize itself with the principles and contextual elements set out in this report, which could serve as a common framework.

The group can then determine needs, both from the organizational perspective, but also according to **realities on the ground** such as professional practices, habits and concerns, based on user knowledge. This approach can be used to identify the constraints as well as the elements of effective solutions put forward by stakeholders on the ground. During this phase, it's important to remain focused on the **expressions of needs**, seen through users' eyes, and not be too hasty in embracing IT-based solutions. The aim is to develop a comprehensive response to the situation in which IT-based tools would be used.

With the organizational needs identified, the **typology of technologies** available and the examples presented in the previous sections could help in selecting the option to implement.

Once a process is outlined and a technological solution chosen, the **matrix** in Appendix 2 could **help validate these decisions**. Note that this tool designed for the purposes for our approach with the members of the ITechLaw association and collaborators of the Human Technology Foundation is not only intended to assess the legal risks associated with the implementation of a project, but also to strengthen good governance practices and to support effective and ethical decision-making. The aim is to encourage decision-makers to **ask the right questions from the outset of the project** and provide both a big-picture and a granular view of the technology under consideration. The process rolls out in seven steps, corresponding to the ethical values discussed below. Each step identifies questions that allow the proposed system's suitability to be assessed against the imperative of serving both the public interest and users' needs.

The more **inclusive** the governance body using this matrix, the greater the diversity of aspects considered in the solution. It will thus constitute a tool for achieving objectivity and a single forum of discussion for stakeholders from different backgrounds.

The proposed matrix is deliberately very detailed, in order to meet the needs of large organizations implementing complex projects. However, it can be used in a simplified format, if the seven steps of the process are implemented carefully:

1. Ethical Purposes and Societal Benefit
2. Accountability
3. Transparence and Explainability
4. Fairness and Non-Discrimination
5. Safety and Reliability
6. Open Data, Fair Competition and Intellectual Property
7. Privacy

The first two columns of this matrix describe the technology under review together with the related potential ethical issues. We recommend these two columns be completed first, for evaluation by governance body members. The implementation of a technological solution always involves making **trade-offs** and **prioritizing** the principles that should be followed. This approach leads to the definition of a framework of common rules and may include constraints or restrictions, which must be accepted and built in to be **effectively applied over time**.

If, in the course of this process, sticking points remain, the "mitigation measures" column makes it possible to study ways of making these constraints acceptable to all and eliminate difficulties through dialogue. The approach can be carried out for several solutions under consideration, with a comparison of the "issues and risks" columns to help separate them and choose what is most appropriate.

Once the decision has been made to deploy a solution using an IT-based device, this matrix can be used at each iteration of an agile process, in order to monitor the sticking points. The matrix can also provide the key messaging elements for ensuring a wide adoption of the solutions by its users.

For implementation in a business organization, please refer to the specificities described in the framed text below.

GOVERNANCE BASED ON KEY PRINCIPLES

The choices made by different states, companies or organizations with regard to COVID-19 tracking applications are therefore not benign and are based on policies and orientations around both technology governance and governance of the health crisis itself. Accordingly, an ethical viewpoint that highlights the values or principles applied (voluntarily and explicitly or not) and their implications for the way these applications are designed, deployed and implemented can provide us with useful insights faced with the difficult choices that entrepreneurs and public decision-makers must make in these times of crisis and, often, urgently.

The **collective crisis governance model we are calling for is based on a set of values** that we believe are relevant to analyzing the various technological solutions, particularly those based on tracking:

Each of the six ethical values presented below are applied at a practical level in the criteria of our multifactor matrix as well as in the methodology discussed above.

Using primarily public documents, members of the ITechLaw association and collaborators of the Human Technology Foundation have applied the multifactor impact matrix (see Appendix 2) to all of the eleven applications under review: DP-3T, TraceTogether, COVI App, ROBERT, Apple/Google API, Aarogya Setu, COALITION, NHSx, Corona-Datenspende, TerraHub and Estimote. We then applied the matrix to produce a document summarizing the key findings observed by the teams. Three examples of summarized key findings can be found in Appendix 4. A comparative table of the eleven applications is provided in Appendix 3.

Accordingly, we have **analyzed** each principle at **two levels**: firstly, the basic legal-ethical concept; and secondly, the framed text shows the operational variations of each principle with illustrations from our multifactor impact matrix of the eleven applications (whether or not they appear positive).

1. ADDED VALUE IS BEYOND DOUBT THE FIRST CRITERION TO BE CONSIDERED, although the meaning of the term covers a variety of ideas as to the expected benefit of an IT-based system. No point of view should be favoured over another, at least initially, but all of them should be considered before any decision is taken. Added value is measured above all in terms of public health and presupposes the comparison of various IT-based as well as non IT-based methods. Then, their contributions — separately or in combination — to combating new transmissions must be considered. This added value is also assessed in economic terms of the direct or indirect costs associated with implementing and operating contact tracing, and when calculating the impact of a persistent pandemic on economic activity. Added value is also assessed in terms of the population's psychological well-being. This value is reflected in criterion No. 1 of the multifactor matrix (Appendix 2), some illustrations of which are provided in the framed text that follows.

ETHICAL PURPOSE AND SOCIETAL BENEFIT

Corona-Datenspende translates into English as "coronavirus data donation," which is what the application is all about: German citizens are encouraged to donate, on a voluntary basis, their data from fitness trackers or health applications, not for any direct feedback on their personal health status, but solely for societal benefit and to support scientists in their work. In terms of the Ethical Purpose & Societal Benefit, the application or, at least, the idea behind its deployment is: since analyses are carried out using the data collected through "Corona-Datenspende," the application could help foster people's impression that each person counts and that each and every citizen can do their part in mitigating the pandemic. In a broader sense, the public discussion about donating one's data may also work as a trigger to strengthen people's perception that their data actually are of value, not only for scientists but for every governmental or private entity seeking to obtain data, and that "donating" one's data should be carefully thought through.

The UK's **NHSx App** currently undergoing beta testing on the Isle of Wight (a small island off the southern coast of England which is part of the British Isles) is based on the user's self-diagnosis (which may be confirmed or not). It uses information about proximity encounters (the Transmitted IDs, i.e., encrypted "Sonar" ID, together with a timestamp for the encounter, and radio signal strength indicator information) uploaded by users either when they have (a) "self-diagnosed" as infected (based on their presentation of symptoms assessed in the tool) OR (b) they report they have confirmed results that they tested positive for the virus. The information provided should reveal to the centralized backend "Sonar" server the devices that were in close proximity to one another, the duration and the distance of that proximity. The UK is currently undecided as to whether to adopt a centralized or decentralized application. Coupled with this is the recent decision by UK authorities to implement manual contact tracing prior to finalization of the application itself (when this had always been viewed as a complementary activity). In this event, it seems likely that the application would be reduced in its effectiveness and consequently in whatever form it is deployed, its ethical purpose and societal benefit will be in doubt.

The **COVI Canada App** is a decentralized contact tracing and risk assessment mobile application developed by a consortium led by the Montreal Institute of Learning Algorithms ("MILA"). The application is designed to provide contact tracing among users, to assess their risk of COVID-19 infection and provide them with recommendations in relation to current behaviour or changes in risk level. It also aims at providing governmental authorities with aggregated information about contagion risks to assist them in designing more effective responses to the pandemic. Like other contact tracing applications, it is estimated that the COVI App will require an uptake rate of 60% of the general populace to ensure efficacy and accuracy of the AI-aspect (aggregate data, epidemiological models, etc.). Nevertheless, for COVI's unique AI-enhanced features (aggregate data, epidemiological models, etc.), MILA estimates that the minimal percentage of download required is much lower, namely approximately 10%. Accordingly, in theory the app should provide a societal benefit, even if adoption rates do not hit the 60% population threshold required by most contact tracing applications.

2. TRANSPARENCY IS ESSENTIAL TO DEBATES ON ETHICS. How do you discuss what might be right and good if you fail to understand the pros and cons involved in the discussions. In the case at hand, this means educating the public at large, on the issues in a debate that is certainly technical but ultimately political, involving citizen behaviour. What are the IT-based solutions? What are the alternatives? Who are the actors behind each solution? Who manages the system, with what data and how? So, in discussing a Bluetooth solution, it is important to know which population the solution is suitable for or which population will be excluded from it. With what risks of error? The efforts of certain research organizations to give an open access description of the specifics of its technological solution are commendable. It is the duty of the government or an independent commission of experts from various disciplines to provide this information (in a simplified and accessible format) — not to make decisions but to respond to requests from all sides and to promote an authentic discussion of ideas among the whole population. This value is reflected in criterion No. 1 of the multifactor matrix (Appendix 3), some illustrations of which are provided in the framed text that follows.

TRANSPARENCY AND EXPLAINABILITY

In this regard, our analysis shows that the **COVI App** is notable from a transparency and explainability perspective. First, in order to help ensure that key components of the terms and conditions are well understood by users, not just agreed to haphazardly, a multi-layered, "progressive" disclosure approach will be adopted. For example, a graphic-heavy top layer illustrating privacy implications can link to a somewhat more textual second-layer — this can then link to the longer FAQ section on the website, which in turn sends users to the full privacy policy. Second, according to the COVI App, user comprehension is verified rather than assumed: "*[MILA will] apply in-app analytics to estimate users' comprehension — for example, by looking at the average amount of time each user has spent looking at various layers of disclosure information. Second, we administer dynamic comprehension quizzes to a random sample of users, allowing us to understand what information has and has not been internalized. Finally, disclosure tools are iteratively revised based on the feedback from these measures, to ensure they best cater to actual user behaviour.*" Third, the output of the model can be explained and decisions can be audited. The user does not receive specific information as to how the risk assessment is calculated. The user will only receive personalized recommendations and tips that are updated as more information becomes available. Fourth, MILA will make available a web page dedicated to this app (where the privacy policy will be available to app users) that explains how individuals may submit a complaint about the handling of their personal information in relation to the app.

The **Aarogya Setu App** is a mobile application developed by the Indian government with private partnership to provide health related information and carry out contact-tracing based on the users' Bluetooth and GPS location data. Responding to pressure from citizens, researchers and civil society groups, the government recently changed its position on two controversial features of the app. The first was the lack of transparency arising from the fact that the app was not open source. In the past, there had been news reports of ethical hackers pointing out security issues in the solution, which had been disputed by the solution's developers. However, it was difficult to comment on the veracity of the claims of either side without the solution's code being audited by multiple independent researchers. The government has now initiated the process of trying to fix this, starting with the release of the app's client-side code for the Android platform and launch of a bug bounty program to encourage improvements to the code. It has also announced that the iOs version and the server code will be released subsequently. Further, the terms of use of the solution have also been modified to remove the prohibition on reverse engineering of the solution. Complete openness in the solution's code is necessary to facilitate audits by independent third parties so as to assess whether the data is indeed being processed in the exact manner stated by the government.

3. AUTONOMY AND RESPECT FOR PERSONAL CHOICE MUST BE AFFIRMED. Expressed in law through the concept of privacy, this ethical value must not mean the single-minded pursuit of self-centred choice but rather the need for a capacity for self development. A democratic society has a duty to guarantee this ability such that this development constitutes a guarantee for everyone of full participation in democratic life. This view of autonomy thus prohibits pitting individual and collective interests against each other, but sees each as linked to other, in a dynamic relationship. Autonomy underlies the responsibility of every individual to work for the common good. We might add that pursuit of the common good cannot stop at national borders but must extend into a global solidarity imposed by the disease. This value is reflected in criterion No. 7 of the multifactor matrix.

PERSONAL DATA AND PRIVACY

"Apple/Google Contact Tracing API", in short "**Apple/Google API**", is a comprehensive solution that includes application programming interfaces (APIs) and operating system-level technology to assist in enabling contact tracing. To strengthen privacy, this protocol leverages a new concept — Bluetooth pseudorandom identifiers, referred to as Rolling Proximity Identifiers. Each Rolling Proximity Identifier is derived from a Rolling Proximity Identifier Key, which is in turn derived from a Temporary Exposure Key and a discretized representation of time. The Rolling Proximity Identifier changes at the same frequency as the Bluetooth randomized address, to prevent linkability and wireless tracking. Non-user identifying Associated Encrypted Metadata are associated with Rolling Proximity Identifiers. The broadcast metadata from a user can only be decrypted later when the user tests positive.

The **ROBERT** (ROBust and privacy-presERving proximity Tracing) protocol was initially a proposal for the Pan European Privacy-Preserving Proximity Tracing (PEPP-PT) initiative, whose main goal is to enable the development of contact tracing solutions compliant with European standards in data protection, privacy and security, within a global response to the pandemic. It has to be noted that, for the time being, "StopCOVID", supported by the French government, appears to be the only application built on the ROBERT protocol. It has been reported that many other countries that were said to be backing PEPP-PT have now moved to DP-3T, using a decentralized structure instead of the centralized ROBERT approach. Some of the initial developers of the PEPPP-PT are also reported to have abandoned the project due to concerns about centralization, transparency and privacy protection.

The **Estimote** wearable transmits and scans for other wearable devices. If the system detects that two (or more) wearables are too close to each other, that is, they are not complying with social distancing guidelines, then the employees are notified via their wearable, such as with a flashing light and an audible beep that gets louder and faster the closer the employees are to one another. Estimote has not updated its Terms of Use or Privacy Policy since 2015. So, although it states it that the solution was built with privacy in mind, Estimote's policies clearly do not support that conclusion.

4. SOCIAL JUSTICE must not be set aside at a time when, in the face of disease, vulnerability is not the same for everyone, demanding that technology be made accessible to all and, first and foremost, to the most disadvantaged. The use of automatic tracking systems excludes people who do not have mobile phones or cannot use Bluetooth; predictive artificial intelligence systems may lead to stigmatizing certain categories of people suspected of being affected by the virus or certain neighbourhoods where infected people reside (usually members of already marginalized groups). The aim must not be simply to protect individuals' data but to avoid discrimination against groups of people. Finally, the value of dignity disallows constant surveillance and public targeting of people with the disease (the coloured QR codes used in China). These values must be taken into consideration from the outset in designing IT-based solutions and throughout their lives (ethics by design). This value is reflected in criterion No. 4 of the multifactor matrix.

FAIRNESS AND NON-DISCRIMINATION

The Indian government's contact tracing tool, **Aarogya Setu**, already has more than 114 million registered users. In relation to the overall population of a country with 1.3 billion inhabitants, this figure could be put into perspective by explaining that this represents only 8.7% of the citizens. The government recently announced that adoption of the app has to be on a "best effort basis" for private workplaces, diluting its earlier position on mandatory adoption, but its use is still mandated by many employers and in contexts like train and air travel. Given the mandatory nature of the tool in some contexts and the potential sanctions that might ensue, one cannot help but notice that the number of people affected by these measures alone exceeds the number of inhabitants of France and Singapore, taken together. This is a risk of discrimination on a large scale, leading to situations where employees/individuals would have no choice but to install the solution or stand the chance of losing an employment opportunity. While a committee set up by the government has issued a protocol to govern the use of data by the app, the lack of a comprehensive data protection law and legislative support for the solution raises concerns about the legal implications and the risk of harm to users. In addition, there is a general risk of surveillance-related use, false positives and negatives and unauthorized access to data (including health data) by third parties.

Estimote is a very simple wearable device. No app is needed, and thus it does not tie up the wearer's phone, nor does it (likely) contain any personal information of the wearer. It can also easily be used by those with disabilities or who are not tech savvy. It merely requires the pressing of a button to indicate infected status. It also has alerts, both visual and vibrations, to let the wearer know that they are not complying with social distancing guidelines (they are too close to one another) and/or that they have been exposed to an infected individual and must then take appropriate measures.

Note that some additional criteria could have a significant impact on fairness or non-discrimination, namely: (i) the content of the notifications, (ii) sanctions (if any) for non-compliance (including, but not limited to, legal sanctions, but also related to the return to work, especially after a period of authorized absence), (iii) limitations on compliance and non-compliance (e.g., financial constraints and socio-economic circumstances).

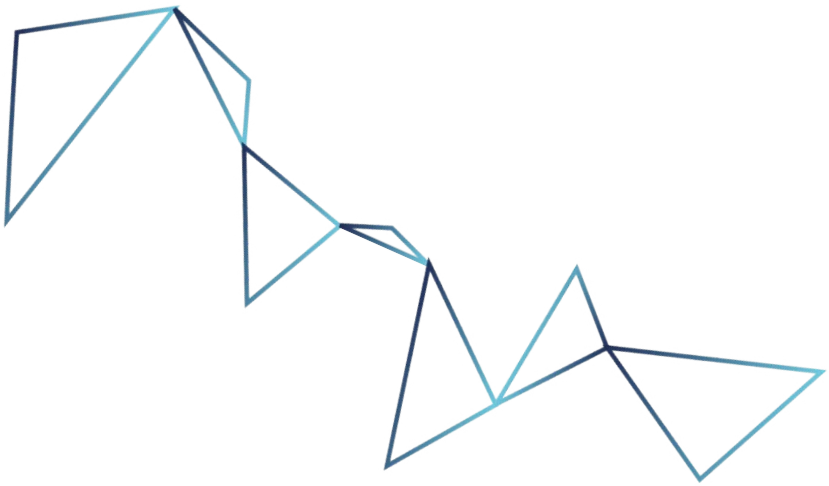
TerraHub has developed a blockchain solution that allows employees to share health information or certificates on a voluntary basis. A proprietary algorithm is then used to analyze these elements to provide the employer with a binary "OK" or "NOT OK" summary result to accompany post-confinement economic recovery measures. This operation legitimately raises questions in terms of transparency and explainability. On the one hand, there is no guarantee that the employee can access the operating mechanisms of this algorithm, so it seems difficult for the employee to understand the underlying criteria that led to an "OK" or "NOT OK" result, and therefore possibly to challenge them. This could, on the other hand, lead to important consequences if this algorithmic decision support tool determines, for example, the conditions of access to the workplace (obligation to stay at home in the event of a negative result, what additional measures will be taken in the event of a positive or negative test, etc.), not to mention the risks of false positives and false negatives. In addition, the secondary use of these data, both "OK/NOT OK" reports and personal data stored outside the chain deserves a clearly defined framework to avoid any misuse by third parties.

5. ASSESSING WHAT IS IN THE PUBLIC INTEREST MUST BE INCLUSIVE AND INVOLVE ALL STAKEHOLDERS. It is important that room should be made for public discussion in a forum that brings together all stakeholders: the medical profession, representatives of civil society (especially vulnerable or marginalized groups), business, education, etc. Decisions around choosing one system over another cannot be left to experts alone, but rather choices must be open for discussion and assessed at both the technical level (ethics by design) and other levels (psychological, socio-economic, etc.). In the end, it is up to the constitutionally designated competent political authority, after hearing the opinions of the required "independent" bodies, to determine and set the parameters and mode of operation of any IT-based tool. To achieve (and maintain) full transparency and public confidence (including how to prevent secure technologies from becoming security technologies), the public authority must explain, minimizing as much as possible the use of patronizing language, the reasons behind the choices made and the details of the decisions, including any AI algorithm models used. In this regard, we must not accept technology choices dictated by actors who might not operate transparently and have no interest in assessing issues of ethics. This value is reflected in criteria No. 2 and No. 6 of the multifactor matrix.

ACCOUNTABILITY

The pseudonymized data necessary for training predictive statistical and epidemiological models for the COVI App will be stored in a secured server with restricted access to selected AI researchers who will train these models. To manage these data, MILA is in the process of setting up a COVI Canada not-for-profit data trust. According to the COVI White Paper, "The data trust would have open rules about its governance, open access to the code and aggregated epidemiological models, and would be continuously monitored by its board, internal experts committees, and external evaluations from independent academic groups and governmental representatives, to make sure that it stays faithful to its mission. It would be dismantled at the end of the pandemic, and all personal data destroyed. The data trust would be in charge of determining who could access the data, and only towards its mission, i.e., to better serve the health and privacy of citizens by managing or doing research on that data. The single mission and non-profit nature of the data trust, as well as the mechanisms to monitor its decisions would be a strong defence to make sure the data does not end being used by companies or governments for surveillance."

The COVI application is an IT-based tool for a post-COVID risk management strategy developed by an independent non-profit organization made up mainly of researchers and not a private company. However, NPO does not necessarily mean absence of private interests. Also, for this approach to be beneficial, it would have to promote greater transparency of the technical characteristics and algorithms used by the application, a principle that is a central issue for digital tools. This transparency will also be enhanced as this is an open source application and since the developer shows a clear concern for the responsible development of products resulting from artificial intelligence. The application's developers have also agreed to have the COVI application evaluated by multiple external parties, including a specially constituted ethics committee, the Commission d'éthique, science et technologie (CEST) of Québec and researchers from the International Observatory on the Societal Impacts of AI and Digital Technologies (OBVIA). This is essential for transparency. Moreover, the openness to external evaluations and the fact that the application has been developed by an interdisciplinary team including experts in technologies and health, promotes the best possible consideration of the various contextual and societal issues that could arise from its use.



The contact-tracing **Coalition App**, developed under the lead of US company Nodle, offers a COVID-19 positive/negative self-declaration service. Users declare themselves "positive" and may choose to notify their condition to the system. Unlike other solutions, this is not necessarily done with the intervention of a health authority or even the need of a test, according to the current information, which may lead to notifications made in error or even maliciously. This is all the more important since this self-declaration triggers notifications to contacts.

OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

TraceTogether is a Bluetooth-based application developed by the Singapore Ministry of Health running on the BlueTrace protocol with the aim of assisting and increasing the effectiveness and efficiency of contact tracing. The BlueTrace protocol is open sourced and the Singapore Ministry of Health has indicated that any other jurisdictions are free to implement locally as they deem appropriate. In fact, this includes the COVIDSafe application launched by the Australian Government Department of Health. In the context of the pandemic, this example shows the value of open source licensing models and interoperable technologies.

DP-3T is a decentralized protocol for a contact tracing app hosted on Apple (iOS) and Google (Android) smartphones which is designed to facilitate contact tracing in the general populace. It proposes an architecture that is capable of international deployment. DP-3T has been released on an open source basis. Data classes are compact ephemeral IDs which are capable of being transmitted via BT LE protocols. Full publication has taken the place of system architecture to enable this portability. Given the need to assess actual national implementations of DP-3T, we are unable to review actual interoperability standards. However, the approach taken by the authors of the protocol itself shows exemplary sharing of data and standards.

6. PROPORTIONALITY AND SECURITY OF IMPLEMENTED SYSTEMS. This value must guide the choice of technology-based systems, if that option is selected. In this respect, the principle of minimum data collected both in terms of content (e.g., in the case of a centralized database, should the national register number of infected and in-contact persons be recorded? Should the name of the doctor who diagnosed the infection be stated?). The quality of data collected and processed and above all the limits on the duration of processing operations will be emphasized. The temptation to preserve the IT-based systems implemented to deal with the emergency of the moment is great. The perpetuation of solutions implemented in the heat of a crisis (the September 2001 terrorist attacks of may be cited here) is often justified in the interests of innovation and the considerable effectiveness that technology can offer legislation. The need for strict compliance with the purpose for which systems are set up must be guaranteed. This implies that the management of health crisis systems exploiting personal health data should be entrusted to bodies bringing together health professionals and stakeholders (e.g., patient groups). Compliance with these principles can be ensured only by giving citizens the right to verify compliance. Lastly, the safety and reliability of the solutions is a crucial point. Indeed, if the solution can be easily pirated or manipulated or if it does not work as intended or is used for non-consensual purposes, then acceptance and trust in the solution will be largely undermined. This value is reflected in criterion No. 5 of the multifactor matrix.

SAFETY AND RELIABILITY

In the case of **Corona-Datenspende**, third parties who know the pseudonym of a data donor could retrieve their authentication token from the RKI server and send further data to the RKI under that pseudonym, including, for example, the number of steps taken or other activity data. Third parties can also connect their own fitness tracker and thus their health data with the pseudonym of another user. These risks must not be considered as simply theoretical because they do not require high-level technical skills.

We would recommend imposing additional safeguards on data deletion. The **DP-3T** proposal currently recommends that data be deleted from servers after 14 days, and the solution itself will "gracefully" and organically disassemble itself when no longer needed as users will stop uploading their data to the Authorization server, or stop using it per se. Our proposal is that a "sunset" provision be added such that data are automatically deleted when an external agency (such as the WHO) declares the pandemic over.

ADOPTING INCLUSIVE AND PARTICIPATORY GOVERNANCE

Beyond the debate on the intrinsic effectiveness of each IT-based solution as a pandemic prevention tool, note that given its nature, the risk may be countered only through a **collective effort**. No anti-COVID-19 tool will therefore produce the expected results if it is not part of an inclusive and participatory public governance approach that makes all the populations concerned accountable and also reassures them. It is not up to the government alone or to individuals, professional unions or companies to impose their solutions without broader consultation and coordination; otherwise, they could be ineffective.

This need for participatory and inclusive governance of IT-based solutions must be rapidly put on the agenda at all levels of civil society: companies, public institutions, intermediary bodies, governments. Indeed, the risks and consequences of sterile opposition between "individuals" and the "state," "businesses" and "public institutions," "federations" and "administration" are too important not to consider **the role that intermediary bodies could play at their respective decision-making level**. While such a need had been expressed before the current crisis, it is now acquiring visibility and public attention unprecedented in the history of our democracies in the digital age.

But what is meant here by governance? Focusing on decision-making processes focuses not so much on the choices to be made as on **how we make those decisions and imagine those actions**. While war or terrorism have, in the past, made it possible to justify the use of exceptional powers, the present health crisis offers the possibility for the mindset of care (see Chapter 1) and an ethic of caring.

The current crisis can therefore be seen as an **educational opportunity** to strengthen the capacity of individuals, groups and communities to become involved in making decisions that affect them. Such a process will enable citizens to better adapt to changing circumstances, and to contribute towards making our society more resilient to face future crises.

This very active and participatory concept of governance should be deployed at several levels. First, at **the political level**, to manage the crisis. In this respect, countries have used different approaches, ranging from interventionism to a certain laissez-faire approach. While rapid and coordinated intervention often led to better control of the pandemic, the initiatives that subsequently led to more effective crisis management seem to have been those where the communities and professional groups involved (intermediary bodies) were listened to. Putting aside the representative aspect resulting from democratic elections and the option not to adopt a proposed action, when citizens play an active role based on choices informed by the different expectations and realities on the ground, they can energize social and political life.

While playing a central role in taking rapid decisions and coordinating actions at the national level, **governments must also encourage local and sectoral initiatives** — whether through crisis management committees in various professional groups to promote economic recovery. In this way, governments can ensure that their guidelines and policies are constantly adjusted with feedback from these initiatives. In Québec, for example, many expert or consultation committees were set up to manage the health crisis, to ensure better alignment between national guidelines and local actions. Difficulties were observed when these groups did not feel sufficiently involved or were not mobilized, or when the authorities announced guidelines and measures that were not supported by their work and recommendations.

The participatory aspect of governance can also be deployed in the way we make our **IT-based choices**. In this report, we have looked at the specific case of tracing applications proposed in different countries and by different developers. In all instances, special attention is given to the individual's choice to consent or not to consent to using the applications in question and transmitting personal data. The adoption of an **inclusive governance** process will, in our view, ensure **voluntary buy-in** by the populations concerned to the use of an IT-based tool. We therefore believe that this approach is incompatible with the choice by some governments to make the use of applications mandatory.

Accordingly, our study showed that most initiatives rely on obtaining consent to justify adequate protection. Can this consent really be considered free and informed? Under social pressure to use such applications, whether in the workplace or in an apartment building, the agency of the person concerned and the "true" voluntary nature of the adoption of technical solutions will have to be questioned. Some informed commentators indicate that this could be at most an induced consent.

Therefore, besides studying each digital application, our broader relationship to the technology must also be examined. The current crisis is thus leading us to (re)consider our entire **technological governance**, i.e., our policies as to when and how to manage IT-based tools in our societies and organizations. It is therefore a question of implementing mechanisms for initiating discussions on the social relevance of available technologies, and when they are deemed desirable, to define the boundaries of social acceptability with respect to them and to develop the values, principles and guidelines for governing their use.

The **earlier this inclusion takes place, i.e., when a technology is emerging**, by questioning its "why" before considering the "how", the more capable we will be to integrate into design choices a wide range of concerns, both for public health and for users, who may be end consumers as well as collaborators or communities. Inclusiveness at the early stages of a technology's development allows us to anticipate problems or challenges that would necessarily arise later and minimize complications resulting from adjustments at more advanced stages. That said, not all issues can, of course, be identified in advance, and it will also be important to ensure feedback throughout the life cycle of the selected technology, to enable constant adjustments for practical issues raised by the use of a technology.

That is the best sense of what we call ethics by design; a notion that goes far beyond the mere statement of general ethical principles to be respected and covers a much broader field than privacy by design. The aim here is to allow for the **contextualization of technological choices and to consider the multiplicity of ethical consequences and issues** they entail. In this respect, the current situation highlights the fact that a health crisis, which calls for **care and solidarity**, may lead to a review of the **priority given to certain values**. It has, for example, been pointed out on many occasions that compromises on tracing applications deemed acceptable in some countries would not be so in Europe or North America, because of possible infringements of freedoms.

The risk of dogmatically pitting individual rights and freedoms against public health needs and the protection of a collective interest remains real and constitutes a trap, particularly in modern Western culture which values the individual. Conversely, groups – families, communities, institutions – always have the authority to restrict their members' rights and freedoms (for example, by citing the common good, such as public health), provided they demonstrate necessity and proportionality. Such political measures are common in certain countries, where curtailment of individual rights and freedoms is not rare. Faced with what is presented as a dilemma, we believe that we must rely on collective intelligence and adopt what we have called the standard of care to walk the narrow path between the two extreme positions. Recent polls show that, in the current context of pandemic, some citizens would be willing to make compromises to ensure the health and safety of their loved ones and seniors. This does not mean that they are ready to give up on their personal freedoms. It implies the need to respond creatively to the challenge of **defining public health and safety with respect for individual freedom and privacy** so they strengthen each other mutually. In the context of a pandemic, this means rethinking IT-based tools to increase collective (health) security that incorporate robust privacy and data safeguards, while incorporating concerns for fairness and social justice. If we can meet this challenge, this new collective security will mean more individual freedom.

In all instances, definitive choices must be avoided and instead use a reasoned, transparent and iterative process to allow for an ongoing evaluation of our technology choices. Trusted third parties, such as **independent verification or certification bodies**, could be usefully involved in such monitoring. Their action should then comply with the policies identified through the mechanisms for stakeholder participation in the governance of the solution.

IMPACT OF COVID-19 ON BUSINESSES

While we do not have sufficient hindsight to analyze the consequences of COVID-19 on the business world, shifts have occurred and must be considered when guiding the choice and implementation of IT-based crisis exit solutions.

With this epidemic, more than just a few isolated individuals have been affected by the fragility of the working world; the entire workforce has been prevented from carrying out its daily work under normal conditions overnight. Those who promote automation and robotization have seen the impact of the pandemic as confirmation of **theories calling for the replacement of the fragile human factor**. While no area seems to be immune to partial or total automation, the immediate reality is quite different in that the core operations of the businesses hit by the virus have been able to survive only through the work — often "invisible" — of some of the least valued occupations. Moreover, in view of the prospects of an unprecedented rise in unemployment in the coming months, or even years, the choice of fully automated systems is likely to provoke strong social tensions. Lastly, note that the **apparent automation of human tasks sometimes simply displaces or conceals human work**.

But the pandemic has also highlighted the fragility and vulnerability of **lean management, zero stock and just-in-time theories**. Tight global supply chains have shown, as the image of the chain suggests, that the snapping of a single link produces a domino effect with global impacts. The extreme fluctuations in demand, whether higher (masks, respirators) or lower (tourism), have suddenly derailed the rules of free trade, to the point that some states — including the most liberal — have had to take action to set prices. There is no doubt that the **issues of relocation and reindustrialization** and their social impacts are going to be intense for all the world's economies, against the backdrop of the desire to regain economic and technological sovereignty, with far-reaching geopolitical consequences.

In this crisis, the theory of **"creative destruction" is likely to have many applications**. The automotive sector, for example, which has already been disrupted for several years due to changing consumption patterns and a loss of reputation as a result of various business issues, is already seeing an acceleration of its "reorientation" with the crisis not yet over. Like other sectors that were the flagships of powerful

economies (air transport, aeronautics, distribution, etc.), the education sector itself, with its sudden and more or less successful shift towards remote teaching and research practices, will also undergo profound changes. Similarly, public services that have been subject to privatization, sometimes excessively so, will also obtain a clearer definition of their real collective challenges.

But the most immediate and massive phenomenon for the economy remains the sudden generalization of remote working. This is not a new subject, but the global scale of the shift to remote working touches the core of the value and social representation of work that has definitively marked a profound change in the organization of salaried work, inherited from Fordism. Numerous testimonials speak to the productivity gains resulting from the elimination of transport time and a more rigorous organization, linked to digital modes of communication. Discovering colleagues and customers in their family environment may have contributed to closer ties. However, many point to the **lack of time for socializing** and face-to-face meetings, which diminishes the sense of belonging to a team and the serendipity necessary for innovation processes. In this new way of doing things, the methods for controlling employees who are "at work", which are the result of Taylorism, are no longer acceptable and a deep rethinking of the organization of businesses is called for, to adapt them to this period of crisis. Needless to say, the effects of these changes around practices are unclear but, by breaking up some of the regulatory frameworks and social consensuses, they are shifting the balance of power by increasing the strength of employers, who can increase their profitability and move gradually towards a platformization of work relationships.

The coming months and years will usher in a completely new reality. Whatever the outcome, which is impossible to estimate at this stage, the notion of **individual and herd resilience** will be essential. In light of human history and development, our ability to act collectively and therefore politically in the face of limited resources has always been our asset. More than ever, **the ability of economies to survive will rely more than ever on the human capacity to act together, no doubt by reimagining the tension between productivity and resilience**.

EXCERCISING GOVERNANCE OVER CORPORATE IT-BASED TOOLS

Deconfinement and the return of employees to the workplace give rise to the need for companies to have solutions, whether technical or not, to **protect everyone from infection and ensure trust in each other**, a prerequisite for business to reopen. Previous analyses have identified a range of technologies that can support social distancing measures (see in particular the framed text on Bluetooth/ iBeacon technologies and the presentation of various workplace access applications). Our aim is not to discuss in detail the practical aspects of deploying each of these IT-based tools, but to identify the characteristics of appropriate and effective governance. Furthermore, lessons learned during containment can lead to a willingness to modify processes and work organization in businesses.

The **specific features of corporate governance** must be acknowledged at the outset. Relationships between employees are both closer and often more intense than in society. The return to work is the time for sharing the experiences lived differently by each person amid the coronavirus pandemic. This sharing is not always an easy thing to do, as the period of confinement may have changed people and their relationships experienced remotely. It is therefore important, at the local level, **to create or recreate spaces for dialogue and sympathetic listening** so that everyone can express themselves on the reality they have lived through and, if necessary, on how remote working has changed the perception of their work within the organization.

Clearly, if an employee becomes infected, management's responsibility would be called into question, risking the right of withdrawal, since safety at work will be declared by the employees as insufficient. The measures related to the health crisis are not part of the normal business activity and can affect the health, relationships and even intimacy of individuals. The **employer-employee relationship may therefore not be sufficient to ensure they are adopted** effectively. However, measures deemed inappropriate, unilaterally imposed or too restrictive are at risk of being circumvented. Accordingly, corporate management must, at the same time, **reassure the employees, clients and suppliers** who need to visit the premises while relying on them to apply the measures strictly. Building this **mutual trust** requires an appropriate mode of governance. In the absence of externally imposed rules, such as legislation, guidelines from regulators or professional bodies, a **common framework of standards** must be drawn up and the hierarchy of principles to be applied and the constraints to be imposed will have to be discussed. Indeed, if they have to choose between security and respect for individual freedoms, employees and clients will most likely choose security, the basic level in Maslow's pyramid of needs. However, such decisions will not be made without regret and bitterness, and could tarnish the image of management.

However, **the structures for social dialogue are not adapted to such crisis situations**: even bodies such as the CHSCT in France or occupational medicine rarely (with the exception of a few specific sectors) have to decide on measures that could impact the survival or structural organization of a company. To ensure that these discussions do not undermine the social climate, it seems appropriate to **set up a multi-stakeholder body to manage corporate health crises**. This body will be key for collecting suggested solutions, discussing priorities, analyzing possible strategies and the IT-based solutions envisaged, and above all in adopting the measures decided upon. The experience of the successful management of the health crisis in countries such as Taiwan or Vietnam has shown the importance of using communities and proximity management. Such a project governing body will enable ethical management by design, i.e., from the very beginning of the strategy design, and will help to create, within the company, an authentic ethical culture and concern for the health of others. In addition, it will offer the possibility of implementing **technological solutions designed from the point of view of users**, whether they are employees or visitors to the premises. Thus, for example, if a self-diagnostic questionnaire or temperature monitoring device indicates that employees are unable to access their workplace, they must be taken care of, by referring them to health care facilities that can confirm a diagnosis and treat them, as well as by offering them the conditions for remote working, if possible, or means of subsistence, while avoiding any stigmatization.

Furthermore, the scale of the efforts that will be required from individuals (access control, physical distancing, disinfection measures, etc.) and the nature of the information that could be collected mean that the health crisis management process should be treated as a **project independent of any other security or control measure**. Although companies can be strongly tempted to use the tools implemented to fine-tune human resources management (employee localization, calculation of working times and breaks), the health crisis management process will need to have specific databases, fully segregated and protected. Employee health data cannot be processed by the employer. **The exclusive purpose of the data collected must be guaranteed** to those who give their consent.

Lastly, such a participatory governance process, based on dialogue, will enable **the strategy for managing the health crisis and the return to work to be developed in agile mode**: measures can be tested and evaluated, in full transparency, in order to achieve the optimal situation by successive iterations. Moreover, while allowing the strategy to be deployed gradually, this mode of governance can also reduce the measures and discontinue them when that is possible, since such limitation of duration is an important factor for trust and social acceptability.

CONCLUSION

In view of the many unknowns surrounding the virus and the factors of contagion, our societies must prepare to live with the threat of pandemic. The end of the crisis expected by the public therefore requires shifting from **health disaster management mode to a medium-term risk management process**. IT-based solutions to assist with deconfinement and economic recovery may thus be studied only as part of a broader risk management process that includes health measures, support for potentially infected people, and oversight of different types of economic and social activities.

To avoid being caught up in a tangle of double constraints that would inhibit decision-making, **a trade-off between the values underlying choices and the prioritization of principles we collectively wish to be upheld must be made**, while avoiding focusing the debate solely on respect for privacy. In this exceptional situation, assimilating data collected or used in managing pandemic risk with particularly sensitive data, possibly placed through management agreements in the care of medical institutions, could offer satisfactory guarantees.

We believe the principle of necessity should be favoured: if the usefulness of an IT-based solution is deemed too low in view of its implementation conditions (for example, an application that would require, in order to be effective, uptake by 60% of the population, but whose adoption would be voluntary), it would be advisable either to temporarily change the conditions of its deployment or change strategy by deploying a different technology.

While tracking potentially infected people is the usual way of managing epidemics, and while one application may allow for large-scale deployment, other approaches are emerging, such as the **use of predictive models of pandemic evolution, which make it possible to identify places and situations at risk**. Here again, ethical risks exist, such as seeing certain neighbourhoods or populations (often already vulnerable or marginalized) stigmatized, but they must be put into perspective in terms of the solution's effectiveness in preserving public health. Thus, the debate cannot focus on how to implement a solution without reflecting on the appropriateness of the solution.

Implementing measures allowing for medium-term management is a challenge in societies that have developed a strong aversion to risk. It requires careful support from public authorities. This support concerns, first of all, the **management and sharing of responsibility**: it cannot rest solely on the shoulders of the individual, which could lead to the stigmatization of infected people; however, it cannot be borne solely by the collective, which could result in a lack of accountability among the least vulnerable people, at the expense of social justice.

Any effective solution therefore requires solidarity among committed citizens. This assumes the following:

- The role of the **government as coordinator** in determining public health priorities (for example, whether to open up sectors of the economy, and in determining the characteristics of IT-based solutions and the type of data collected), and in promoting standards that enable national and international interoperability of digital devices. In particular, business leaders, cannot be solely responsible for deciding on deconfinement or operations management measures in the event

of a health crisis (prior to the mass distribution of a vaccine), in the midst of a social dialogue that could become tense. The government will also have to define the adjustments for minimizing the discriminatory effects or harm suffered by certain categories of the population as a result of the use of such measures, for example, by introducing public policies to compensate for the loss of income for persons or communities who declare they are infected.

- The role of standards bodies or independent multidisciplinary advisory groups in assessing the potential technologies and developing standards that consolidate all best practices for the responsible development and deployment of these new technologies and **enabling their national and international interoperability**.

- The **role of the private sector** in the ethical and responsible development and deployment of these technologies and in the overall measures taken to ensure the health of employees and customers, as well as the responsible reopening of the economy.

- The **management role of communities** (municipalities, intermediary bodies, neighbourhood associations, school boards...) in the local application of measures, adapting them as much as possible to the realities on the ground and encouraging the population's buy-in.

- The **role of each citizen** in adopting measures that are sometimes very restrictive, but which can effectively combat the pandemic — which requires individual, collective and equitable responsibility across all stakeholders — and the desire of the vast majority of citizens to avoid catching the virus and infecting their loved ones.

The governance of the selected IT-based solutions therefore appears to be the key factor conditioning their success or failure and must reflect the management of the responsibilities mentioned above. To do so, an appropriate body must be created, which must be:

- **Multipartite:** In addition to members of parliament and the government, who guarantee legitimate regional and national representation, as well as experts, the specific body for governance and control of IT-based solution deployment must also include representatives of civil society and intermediary bodies, capable of inspiring citizen trust and commitment.

- **Agile:** As the situation and knowledge of the virus and how it spreads evolve, the chosen solution will have to be adapted in successive iterations.

- **Transparent and reasoned:** In periodic assessments and possible adjustments to potential solutions, the reasoning process and rationale (or evidence) used must be explained and supported transparently and understandably. This is crucial for stakeholder confidence in the choices made.

- **Temporary:** If the risk of pandemic persists, the evolving and iterative nature of the proposed solutions should allow for their impact to be reduced and then discontinued as required, under the direct control of the governance body.

APPENDICES

NOTE: This PostCoviData Impact Assessment template has been developed by the members of ITechLaw listed in Appendix 3 in the context of the PostCoviData Project led by the Human Technology Foundation. The contributors to this template have participated in its development on a personal basis. Accordingly, the views expressed in this template do not reflect the views of any of the law firms or other entities with which they may be affiliated.

This template is provided for informational purposes only. It does not constitute legal advice. It is provided as an example of the key types of information that can be considered during the PostCoviData Tech Solution Pandemic Impact Assessment process. Adjust it as necessary to fit your needs in consultation with qualified legal counsel.

APPENDIX 1

POSTCOVIDATA IMPACT ASSESSMENT

[Project Owner]
[Project Name]
PostCoviData Impact Assessment ("PIA")

<Day> <Month> <Year>

1. PROJECT SUMMARY

(Describe the Pandemic Tech Solution, the dataset and the context)

In this document, "**Pandemic Tech Solution**" means a software solution, device or product developed or deployed by the Project Owner that integrates data-driven functionalities.

Describe the project and what it intends to achieve by addressing the following key points:

- *Describe the Pandemic Tech Solution as a whole, including a functional description/overview and the datasets.*
- *What does the Pandemic Tech Solution seek to achieve?*
- *What is the political and social context in which the Pandemic Tech Solution would be deployed or used?*
- *Does the Pandemic Tech Solution raise issues of specific ethical concern that should be explored prior to proceeding?*
- *Where does the PIA sit within the project timeline? Is it intended to evolve?*
- *What is the Project Owner trying to achieve with the Pandemic Tech Solution?*
- *Is the Pandemic Tech Solution a one-off initiative or part of ongoing business development?*

Project summary

[NOTE: Is this Pandemic Tech Solution an expansion of a previous activity? If yes, determine whether a previous assessment has been done. If a previous assessment has been done, what has changed in this data activity and why (refer to previous assessment)?*]*

Dataflow chart

Governance structure

2. KEY FACTORS FOR CONDUCTING A PIA

The first step in conducting a supplemental Pandemic Tech Solution Impact Assessment should be an evaluation of why that specific Pandemic Tech Solution requires such a PIA, with regard to any Risk Impact Assessment already conducted.

To conduct this first step, the Project Owner should define clearly the scope and goals of the Pandemic Tech Solution and the characteristics of the envisioned Pandemic Tech Solution. At this stage, many elements need to be considered, but the analysis need not be as thorough as at the main assessment. Important criteria to consider are listed in the Table below (note that this list is non-exhaustive and should be adapted to the specific context of the Project Owner). It should be noted that this PIA will need to be continuously adjusted as the scientific community confirms the pandemic's characteristics. The present PIA will also need to be adjusted based on evolving knowledge about the impact of any tech solutions on individuals and societies.

At this preliminary stage as well as during the main risk assessment, risks factors should be evaluated based on low to high risk scale (low, medium, high). A holistic and contextual approach is recommended. Such an approach should consider the factors in relation to one another. For instance, a Pandemic Tech Solution deployed strictly internally to support certain decision-making processes might be said to be, in general, less risky than a citizen-facing system. However, an internal Pandemic Tech Solution used to evaluate or monitor employees might trigger certain labour laws obligations and in consequence be riskier than certain citizen-facing systems.

Factors Justifying Need For Impact Assessment	Risk Rating (Low, Medium, High)	Commentary
1. What is the context in which the Pandemic Tech Solution will be used or deployed? Would this use be citizen-facing?		
2. Does the country have data protection laws or regulation? How does it fare on rule of law? Is the Pandemic Tech Solution deployed in an exception legal context (state of emergency)?		
3. Will the Pandemic Tech Solution be used across legal jurisdiction borders (whether they be across federal states or country borders)?		
4. Who will be the categories of persons involved in the Pandemic Tech Solution?		
5. What is the type and origin of the data that will be used to train the Pandemic Tech Solution? Will, in the context of an AI solution, the training data include personal information? What is the level of sensitivity of the data? Who are the data subjects?		
6. What kind of decisions will the Pandemic Tech Solution be making? What rights and interests will be at stake? Are those rights fundamental or human rights?		
7. What is the expected degree of autonomy of the Pandemic Tech Solution? Will, for instance, human operators or decision-makers have oversight on individual AI decisions, if any? How frequently will oversight occur? What measures will be made to avoid automation bias or anchoring to the Pandemic Tech Solution?		
8. What are the technical characteristics of the Pandemic Tech Solution that could influence the explainability and auditability of the algorithm? Can the Pandemic Tech Solution be explained?		
9. What will be the Project Owner's degree of control and responsibility over the finalized Pandemic Tech Solution? Who are the expected contributing third parties?		
Synthesis (is this supplemental PIA required/useful and key points leading to this conclusion):		

3. MAIN ASSESSMENT

Each row in the following table summarises the key requirements of responsible Pandemic Tech Solution principles and outlines some key questions or considerations you should address. See the checklists provided in the attached Appendix 1 for assistance in what documents should be consulted and what information should be included in filling out the following table.

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #1: Ethical Purpose and Societal Benefit *Project Owners that develop, deploy or use Pandemic Tech Solution and any national laws that regulate such use should require the purposes of such implementation to be identified and ensure that such purposes are consistent with the overall ethical purposes of beneficence and non-maleficence, as well as the other principles.*				
Overview of the Principle · The Project Owner should review the objectives of the Pandemic Tech Solution, e.g. ensuring consistency in decision-making, improving operational efficiency and reducing costs, or introducing new product features to increase citizen choice. The Project Owner should then weigh them against the risks of using the Pandemic Tech Solution in the Project Owner's decision-making. · The Project Owner should gather the key stakeholders required for the discussion/decision, including: – Internal stakeholders (project manager, chief scientist, officer, board member, employees, civil society etc.) – External (developer, external data provider, research partner, distributor, etc.) – End user (citizen, service user, etc.) – Government (public institution, regulatory agency, etc.) – Members of vulnerable groups requiring special care (children, disabled persons, people with little technological literacy, etc.) In determining the level of human oversight, the Project Owner should consider the impact of the decisions of the Pandemic Tech Solution on the individual, group of individuals and on society in general. On that basis, the Project Owners should identify the required level of human involvement in the decision-making of the Pandemic Tech Solution.				
PART I – GENERAL ASSESSMENT APPLYING TO ALL TECH SOLUTIONS				
1. What laws apply to the collection, analysis and use(s) of data?				
2. Are there other legal, cross-border, policy, contractual, industry or other obligations linked to the collection, analysis and use(s) of data?				
3. May the Pandemic Tech Solution be deemed as medical device or any other qualification that could entail application of other regulation (e.g. medical secrecy) that could modify its ethical perception?				
4. Does the Pandemic Tech Solution comply with the values, standard and policies of the Project Owner?				
5. What are the potential reputational and material risks for the Project Owner?				
6. Will the deployment or use of the Pandemic Tech Solution affect the autonomy of the affected stakeholders?				
7. Consider appropriate safeguards to promote the informed human agency, autonomy and dignity of employees and to avoid inappropriate or destructive impacts on the emotional or psychological health of employees (monotony of tasks, excessive surveillance, gaming of behavior, continuous exposure to horrific content).				
8. Consider any other appropriate safeguards that should be assessed, as time-limit, automatic deletion.				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
PART II – SPECIFIC ASSESSMENT APPLYING TO AI AND MACHINE-LEARNING BASED SOLUTIONS				
9. Consider whether it is achievable from a technological perspective to ensure that all possible occurrences should be pre-decided within the Pandemic Tech Solution to ensure consistent behavior. If this is not the case, consider how the outcomes (aka machine behaviours) will be monitored and fed back into the governance and oversight framework.				
Principle synthesis • *Is the Pandemic Tech Solution compatible with human agency, human autonomy and the respect for fundamental human rights?* • *Does the Pandemic Tech Solution comply with the ethical purposes of beneficence and non-maleficence?* • *What are the risks of harm to persons and their rights of this Pandemic Tech Solution?* – Should notably be considered as a risk factor the possibility given to individuals to decline to install the solution and to uninstall it/remove it from devices. – Should also be considered the proportionality of the collection of device data regarding the aims of the solution. – Should be considered as well whether the Project Owner has implemented effective measures to ensure human control and oversight on the automated decision-making process of the solution, if any. – Should also be investigated the broader impact that use of the solution may have on stakeholders other than the end-user.				
Principle #2: Accountability Project Owners that develop, deploy or use Pandemic Tech Solution and any national laws that regulate such use shall respect and adopt the seven principles developed in the framework (or other analogous accountability principles). In all instances, humans should remain accountable for the acts and omissions of data-driven systems. **Overview of the Principle** — The Project Owner should ensure at all times that it remains accountable for the ethical and responsible deployment of Pandemic Tech Solutions that the Project Owner deploys, including by means of "human-in-the-loop" or "human-over-the-loop" deployment.				
PART I – GENERAL ASSESSMENT APPLYING TO ALL TECH SOLUTIONS				
1. Is the Pandemic Tech Solution centralized or decentralized?				
2. What is the level of internal support, including financial, for the Pandemic Tech Solution?				
3. Who will be accountable within the Project Owner with regards to the Pandemic Tech Solution? Is there a central coordinating body? Who will be accountable within the Project Owner upon failure of the Pandemic Tech Solution, or upon production of adverse outcomes for its users?				
4. What are the roles played by the Project Owner within the Pandemic Tech Solution pipeline (end-user, developer, data provider, etc.)?				
5. Is there an independent commissioner committed to the review and control of such Pandemic Tech Solutions? (e.g. governmental agency, designated official)				
6. Will the staff be trained to use the Pandemic Tech Solution? Are the relevant personnel and/or departments fully aware of their roles and responsibilities? This inquiry should account for different types of staff and the different layers of personnel involved in the design of the Pandemic Tech Solution (e.g., management / oversight in addition to programming levels).				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
7. How will the internal use of the Pandemic Tech Solution by the Project Owner affect the roles and tasks of employees?				
8. What elements of the training and development "supply chain" have been outsourced? If handed off to a third party, are their services subject to the same levels of quality control as the Project Owner?				
9. To what extent does the Pandemic Tech Solution rely on third party data/systems input? How accountable are those third-party dependencies?				
10. Have external QA/QC control methodologies been observed in the creation of the Pandemic Tech Solution (i.e. ISO 9001)?				
PART II – SPECIFIC ASSESSMENT APPLYING TO AI AND MACHINE-LEARNING BASED SOLUTIONS				
11. If applicable, how will the AI model training and selection process be managed?				
12. If applicable, consider maintenance, monitoring, documentation and review of the AI models that have been deployed.				
13. If applicable, consider the various degrees of human oversight in the decision-making process: a) **Human-in-the-Loop:** This model suggests that human oversight is active and involved, with the human retaining full control and the AI only providing recommendations or input. Decisions cannot be exercised without affirmative actions by the human, such as a human command to proceed with a given decision. (NB: Considering here also the concept of "**Human in the Loophole**" where there is automation bias, anchoring or confirmation bias in respect of the human operative. The human essentially affirming the AI outcome without critically assessing whether it is correct or not). b) **Human-out-of-the-Loop:** This model suggests that there is no human oversight over the execution of decisions. AI has full control without the option of human override. c) **Human-over-the-Loop:** This model allows humans to adjust parameters during the execution of the algorithm.				
14. Does the Pandemic Tech Solution involve development, deployment or use of an AI solution or a combination of the three?				
15. What are the rights and interests at stake when the Pandemic Tech Solution makes an automated decision?				
Principle synthesis · Should notably be considered the governance of the Pandemic Tech Solution and whether it ensures the respect of rights and interests of the users. · Should also be considered the safeguards implemented to ensure independence of the Pandemic Tech Solution.				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #3: Transparency and Explainability *Project Owners that develop, deploy or use Pandemic Tech Solution systems and any national laws that regulate such use shall ensure that, to the extent reasonable given the circumstances and state of the art of the technology, such use is transparent and that the decision outcomes of the data-driven system are explainable.* **Overview of the Principle** · The Project Owner should ensure at all times that the Pandemic Tech Solution is transparent, including by means of notifying affected stakeholders of: a) the fact that a Pandemic Tech Solution is being used; b) the intended purposes of the Pandemic Tech Solution; and c) the identity of an individual who can respond to questions regarding the Pandemic Tech Solution. Transparency can be reinforced through the concepts of explainability, repeatability and traceability. · The intensity of the transparency and explainability obligations will depend on a variety of factors, including the nature of the data involved, the result of the decision and its consequences for the affected individual. Project Owners that develop Pandemic Tech Solution should ensure that the system architecture, algorithmic logic, data sets, testing methods, and all related development and operational policies and procedures serve to embed transparency and explainability by design.				
PART I – GENERAL ASSESSMENT APPLYING TO ALL TECH SOLUTIONS				
1. Are clear and readable Terms of Use provided to users of the Pandemic Tech Solution?				
2. Do the Terms of Use include data sharing mechanisms? Are there any inconsistencies between what is stated in the Terms of Use and the identified functioning of the Pandemic Tech Solution?				
3. Is a Privacy Policy available?				
4. Does the Project Owner provide information on the scale of adoption? Is there such information available outside of the Project Owner?				
5. Is the Project Owner transparent about the outcomes of the Pandemic Tech Solution? (e.g. false positive or false negative rates of a contact-tracing app...)				
6. Does the Project Owner know what data is used in the Pandemic Tech Solution and how that data is used to arrive at a decision? Would the Project Owner be able to explain the Pandemic Tech Solution to the public?				
7. Does the original data include proprietary information?				
8. Does the original data include anonymised or synthetic data? Would the Pandemic Tech Solution outcome be more accurate/beneficial/ less risk of bias if it had included personal information?				
9. Does the original data include personal information?				
10. Is the Pandemic Tech Solution auditable? Auditability refers to the readiness of a Pandemic Tech Solution to undergo an assessment of its algorithms, data and design processes.				
11. Is the Pandemic Tech Solution robust? Robustness refers to the ability of a computer system to cope with errors during execution and erroneous input, and is assessed by the degree to which a system or component can function correctly in the presence of invalid input or stressful environmental conditions.				
12. Is the Project Owner able or prepared to undertake an assessment of the Pandemic Tech Solution to identify the cause of any discriminatory or adverse outcome produced by the Pandemic Tech Solution?				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
PART II – SPECIFIC ASSESSMENT APPLYING TO AI AND MACHINE-LEARNING BASED SOLUTIONS				
13. What is the general degree of opacity of the Pandemic Tech Solution? (ie to what degree could it be described as a "black box")				
14. What type of AI model was used to create the Pandemic Tech Solution, if any?				
15. Is it possible for a specialist to understand how the Pandemic Tech Solution makes its decisions and how it reached a specific conclusion in a specific case?				
16. Consider designing the Pandemic Tech Solution from the most fundamental level upwards to promote transparency and explainability by design.				
17. What are the risks for the rights and interests of stakeholders of unexplainable AI decisions, if any?				
18. What are the transparency and explainability expectations of the different stakeholders?				
19. What is the degree of sophistication of the persons due to receive the explanation (AI specialist, lay-person, educated lay-person, etc.)?				
20. How useful would be this data for persons outside the Project Owner to understand the AI system and its decisions? Would end-users be incentivised or able to game the Pandemic Tech Solution, if aware of the solution's decision-making process?				
21. Is the Pandemic Tech Solution explainable? The Project Owner should be able to explain to a third party how the Pandemic Tech Solution's algorithms function and/or how the decision making process incorporates model prediction.				
22. Is the Pandemic Tech Solution repeatable? Repeatability refers to the ability to consistently perform an action or make a decision, given the same scenario. The consistency in performance could provide AI users with a certain degree of confidence.				
23. Is the Pandemic Tech Solution reproducible? Reproducibility refers to the ability of an independent verification team to produce the same results using the same AI method based on the documentation made by the Project Owner.				
24. Is the Pandemic Tech Solution traceable? A Pandemic Tech Solution is considered to be traceable if its decision-making processes are documented in an easily understandable way.				

Principle synthesis

- Should notably be assessed the documentation available to users and the degree of clarity of such documentation.
- Should notably be highlighted any opacity of whole or part of the Pandemic Tech Solution.
- Should also be summarized the choices made by Project Owner regarding datasets used for the Pandemic Tech Solution.

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #4: Fairness and Non-Discrimination *Project Owners that develop, deploy or use Pandemic Tech Solution and any national laws or internationally recognized standards that regulate such use shall ensure the non-discrimination of data-driven outcomes, and shall promote appropriate and effective measures to safeguard fairness in use.* **Overview of the Principle** · The use of the Pandemic Tech Solution should be non-discriminatory in terms of accessibility. The Pandemic Tech Solution should be accessible also to people with disabilities (such as, for instance, limited visual capacity). · Decisions based on the Pandemic Tech Solution should be fair and non-discriminatory, judged against the same standards as decision-making processes conducted entirely by humans. AI development should be designed to prioritize fairness. · This would involve addressing algorithms and data bias from an early stage with a view to ensuring fairness and non-discrimination.				
PART I – GENERAL ASSESSMENT APPLYING TO ALL TECH SOLUTIONS				
1. Is the data high quality data? The following factors should be assessed: – the accuracy of the dataset, in terms of how well the values in the dataset match the true characteristics of the entities described by the dataset; – the completeness of the dataset, both in terms of attributes and items; – the veracity of the dataset, which refers to how credible the data is, including whether the data originated from a reliable source; – how recently the dataset was compiled or updated; – the relevance of the dataset and the context for data collection, as it may affect the interpretation of and reliance on the data for the intended purpose; – the integrity of the dataset that has been joined from multiple datasets, which refers to how well extraction and transformation have been performed; – the usability of the dataset, including how well the dataset is structured in a machine-understandable form; – the usability of any personal information contained within the data sets, including with regards to obtaining any requisite consents; and – human interventions, e.g. if any human has filtered, applied labels, or edited the data.				
2. Consider minimizing inherent bias: – Selection Bias: This bias occurs when the data used to produce the Pandemic Tech Solution are not fully representative of the actual data or environment that the Pandemic Tech Solution may receive or function in. Common examples of selection bias in datasets are omission bias and stereotype bias. – Measurement Bias: This bias occurs when the data collection device causes the data to be systematically skewed in a particular direction. – The following factors should be assessed: · the frequency with which the dataset is reviewed and updated; · the diversity of the dataset, and the variety of sources from which the data has been collected (i.e., numeric, text, audio, visual, transactional etc.); and · the usability of different datasets, including how those datasets have been matched and cleaned so that relational datasets can be correlated and linked.				
3. Is the Pandemic Tech Solution making automated decisions affecting the rights and interests of individuals or businesses – Should notably be considered whether the Pandemic Tech Solution may have consequence for the user to suffer differential treatment which would otherwise be prohibited under any applicable law.				
4. Is the use of the Pandemic Tech Solution voluntary, incentive or compulsory?				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
5. Is there rigorous testing of the Pandemic Tech Solution, both before use and periodically afterwards, to ensure that there is no disparate impact on a protected class of individuals?				
6. May the Pandemic Tech Solution exclude some categories of people from using it? – Have design features contemplated needs of the elderly (for example, ease of use)? – Have design features contemplated the needs of people with disabilities: See: World Wide Web Consortium's Web Accessibility Initiative				
7. Does the Project Owner have in place a system to respond to and resolve situations in which the Pandemic Solution produces discriminatory or unfair outcomes? – This should encompass the Project Owners' capacity to assess and identify biased datasets, potential relief measures provided to end-users and any scope to re-design the Pandemic Tech Solution.				
PART II – SPECIFIC ASSESSMENT APPLYING TO AI AND MACHINE-LEARNING BASED SOLUTIONS				
8. What methodologies have been applied and used in the training of the Pandemic Tech Solution?				
9. Does the Pandemic Tech Solution have a fixed learning phase followed by static use phase or does it continuously improve? If the latter, how are improvements filtered for bias, quality etc.?				
10. What are the risks of bias in 1) the algorithm, 2) the training data, 3) the human developers, 4) end-users?				
11. What are the reputational risks for the Project Owners of the Pandemic Tech Solution making biased automated decisions?				
12. How are "edge cases" managed by the Pandemic Tech Solution?				
13. Is the data used for the training of the Pandemic Tech Solution representative of the population about which the Pandemic Tech Solution will make decisions (data accuracy, data quality and data-completeness)?				
14. Does the Project Owner have an established and robust selection process in relation to the datasets training the Pandemic Tech Solution? For example, are there minimum requirements as to the diversity and quality of the datasets used?				
15. Does the Pandemic Tech Solution use different datasets for training, testing and validation? Weighting Bias: This bias occurs when the data used by the AI Solution are attributed differing weights in producing the relevant outcome. The datasets might be afforded greater or lesser value, which might be arbitrarily or inaccurately awarded.				

Principle synthesis

- Summarize inherent biases of the Pandemic Tech Solution, if any.
- Should notably be assessed any identified discrimination or potential restriction of use for certain categories of persons.
- Should notably be addressed the risk of having derivative misusage of the Pandemic Tech Solution.

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #5: Safety and Reliability *Project Owners that develop, deploy or use Pandemic Tech Solution and any national laws that regulate such use shall adopt design regimes and standards ensuring high safety and reliability of data-driven systems on one hand while limiting the exposure of developers and deployers on the other hand.* **Overview of the Principle** The Project Owner should test the Pandemic Tech Solution thoroughly to ensure that it reliably adheres, in operation, to the underpinning ethical and moral principles and has been trained with data which are curated and are as 'error-free' as practicable, given the circumstances.				
PART I – GENERAL ASSESSMENT APPLYING TO ALL TECH SOLUTIONS				
1. In case the Project Owner does not hold international recognized information security certifications (such as ISO/IEC 27001), what is the current level of the security measures adopted? It should notably be assessed the following measures: security incident detection, response and management, business continuity plans, change management policies.				
2. What is the Project Owner's history of data breaches and incidents? How has the Project Owner responded to data breaches and incidents in the past?				
3. What are the cybersecurity risks and vulnerabilities of the Pandemic Tech Solution? Who is at risk of harm? What preventative measures are in place?				
4. Regarding people accessing the data, is confidentiality ensured?				
5. What are possibilities for subversion of intended use? (i.e. where the technology is capable of "dual use")				
6. What are the safety and reliability expectations of the clients and what are their level of sophistication?[1]				
7. What information relating to secure software development and implementation of encryption measures at rest and in transit are provided?				
8. What are the availability and effectiveness of redress mechanisms?				
PART II – SPECIFIC ASSESSMENT APPLYING TO AI AND MACHINE-LEARNING BASED SOLUTIONS				
9. What are the risks of a technical failure of the Pandemic Tech Solution? What are the risks of inaccurate results, polluted datasets, and misuse?[2]				
Principle synthesis · Should notably be summarized and assessed all the technical and organizational measures taken to ensure the safety of the Pandemic Tech Solution.				

[1] Supra note 11.
[2] Supra note 5.

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #6: Open Data, Fair Competition and Intellectual Property *Project Owners that develop, deploy or use data-driven systems and any national laws that regulate such use shall promote open source and decentralized frameworks. Project Owners that develop, deploy or use Pandemic Tech Solution should take necessary steps to protect the rights in the resulting works through appropriate and directed application of existing intellectual property rights laws.* **Overview of the Principle** · The Project Owner should assess how its Pandemic Tech Solution and its outputs can be used in other pandemic situation or by other Project Owner. · Project Owners must be allowed to protect rights in Pandemic Tech Solution. However, care needs to be taken not to take steps which will amount to overprotection, as this could prove detrimental to the ultimate goal of IP protection.				
1. Is the Pandemic Tech Solution open-source?				
2. Are some use restrictions made clearly public? (e.g. for open-source solutions)				
3. Does the Pandemic Tech Solution offer portability easily?				
4. What is the scope of interoperability with tech solutions offered by other providers?				
5. When developing "heat maps" or related projects, are data sharing is based on anonymized data?				
6. Is the data generated by the Pandemic Tech Solution reusable for other public interest (data for good) projects?				
7. What are the ownership or intellectual property rights attaching to the Pandemic Tech Solution?				
8. Are there any compulsory licensing or patent rights issues relating to the Pandemic Tech Solution?				
9. Have the intellectual property rights attaching to the Pandemic Tech Solution been made publicly available (i.e., turning the underlying code into an open source program)?				
10. Alternatively, are there any obligations or expectations around the provision of the underlying code or software to the public or government entities? If so, will there be any measures regarding adequate remuneration for Project Owners that make such contributions?				
Principle synthesis · Summarize the rights and restrictions attached to the use of the Pandemic Tech Solution.				

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
Principle #7: Privacy *Project Owners that develop, deploy or use Pandemic Tech Solution and any national laws that regulate such use shall endeavour to ensure that data-driven systems are compliant with privacy norms and regulations, taking into account the unique characteristics of data-driven systems, and the evolution of standards on privacy.* **Overview of the Principle** The Project Owner should consider implementing operational safeguards to protect privacy such as privacy by design principles that are specifically tailored to the specific features of deployed the Pandemic Tech Solution.				
1. Are the principles of necessity, proportionality and data minimization fully integrated?				
2. What privacy by design measures have been implemented?				
3. Are personal data that are being collected by the Pandemic Tech Solution used for any secondary purposes during or after the pandemic? Are secondary use of data compatible with initial purposes, if any?				
4. How are transfers of data of the Pandemic Tech Solution outside of the EU/national/regional frontier organized?				
5. What is the Project Owner's lawful basis for processing personal information? What measures does the Project Owner take to ensure compliance?				
6. Who were the data subjects? What type of information was collected about them? What is the scope of the consents obtained?				
7. Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws?				
8. What is the nature of the Project Owner's relationship with the data subjects? How much control will they have? Would they expect you to use their data in this way?				
9. Is sensitive data collected? If so, are there higher standards being adopted for protection of this kind of data?				
10. How was the data used by the Pandemic Tech Solution collected and stored? Was the data transferred by third parties or will the data be transferred to third parties? – Consider whether preprocessing activity has been done on the data before the analysis and whether it would have affected the accuracy and appropriateness of individuals				
11. Are there viable alternatives to the use of personal information? (e.g. anonymization or synthetic data If so, what mechanisms/ techniques are implemented to prevent from re-identification?				
12. Consider if the data is provided by the individual (originated in direct action taken by the individual) and whether: – The data is initiated (the product of individuals taking an action that begins a relationship) – The data is transactional (created when the individual is involved in a transaction) – The data is posted (created when individuals proactively express themselves)				

[3] Ibid.

Factors to Consider for Risk Ranking	Whether/How the Solution Addresses the Factors	Risk Rating (Low, Medium, High)	Mitigation Measures	Commentary
13. Consider if the data is observed (created as the result of individuals being observed and recorded), whether: – The data is engaged (instances in which individuals are aware of observation at some point in time) – The data is not anticipated (instances in which individuals are aware there are sensors but have little awareness that sensors are creating data pertaining to the individuals) – The data is passive (instances in which it is very difficult for the individuals to be aware they are being observed and data pertaining to observation of them is being created)				
14. Consider if the data is derived (created in a mechanical fashion from other data and becomes a new data element related to the individual), whether: – The data is computational (creation of a new data element through an arithmetic process executed on existing numeric elements) – The data is notational (creation of a new data element by classifying individuals as being part of a group based on common attributes shown by members of the group)				
15. Consider if the data is inferred (product of a probability-based analytic process), whether: – The data is statistical (the product of characterization based on a statistical process) – The data is advanced analytical (the product of an advanced analytical process)[3]				
16. Beyond the data subjects' privacy, may the privacy of an identified group be at risk?				
17. Are there procedures for reviewing data retention and performing destruction of data used by the Pandemic Tech Solution? Are there oversight mechanisms in place?				
18. Does the Pandemic Tech Solution provide a functionality allowing the user to "turn-off" the app for a limited time?				
Principle synthesis · Summarize how personal data protection and privacy principles are addressed by Project Owner: – Data subjects; – Categories of data; – Rights and exercise; – Potential conflict with Group Privacy.				

4. RISK ASSESSMENT SUMMARY

This section describes the risks you've identified through the PIA process and how you propose to mitigate and manage those risks. It can be useful to link this back to the principles to show why these risks and the proposed actions are relevant. Document the risks in line with any existing risk management processes the Project Owner has – it will be more efficient than trying to run a separate process.

5. RISK MITIGATION ACTION PLAN

This section describes how you propose to mitigate and manage the risks previously described. In some cases, it may be helpful to categorize these actions into areas such as: **Governance / People / Process / Technology**.

Please provide details of all such strategies. Also, please identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred. You can use the form of table below.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.				
2.				
3.				
4.				
5.				

APPENDIX 2

COMPARISON TABLE OF 11 INITIATIVES

Solution	Communication Protocol/App/ Wearable	Public / Private / NFP	Ethics Review/ DPIA/PIA	Centralised/ Decentralised/ Hybrid	AI/ML Or not	GPS/ Bluetooth/ Other	Self-diagnosis/ Validated diagnosis
1 MILA Covi App	Application	Not-for-profit	PIA	Hybrid: Mostly decentralised with centralised elements	AI/ML	Initially GPS/ subsequently Bluetooth	Validated diagnosis/ AI-developed risk assessment
2 ROBERT	Protocol	Public	PEPP-PT Manifesto[1]	Hybrid: Mostly centralised with decentralised elements	Not	Bluetooth	Depends on application (allegedly self-diagnosis)
3 Corona-Datenspende	Application	Public	None available	Centralised	Not	Connected devices	n.a. (no diagnosis at all)
4 Apple/Google	Protocol	Private	None available	Decentralised	Not	Bluetooth	If diagnosed with COVID-19, users must provide their consent to share Diagnosis Keys with the server
5 DP-3T	Protocol	Public	DPIA	Hybrid: Mostly decentralised with centralised elements	Not	Bluetooth LE	Validated diagnosis
6 NHS	Application	Public	DPIA	Centralised	Not	Bluetooth LE	Self-diagnosis followed by validation. Self declared/ contributed.
7 TraceTogether	Application	Public	DPIA	Hybrid: Mostly decentralised with centralised elements	Not	Bluetooth	Validated diagnosis
8 Coalition	Application	Not-for-profit	DPIA	Hybrid: Mostly decentralised with centralised elements	Not	Bluetooth	Self-diagnosis
9 Aarogya Setu	Application	Public	None available	Hybrid: partly centralised	Not	GPS, Bluetooth	Self-diagnosis
10 Estimote[2]	Wearable device & backend software	Private	Aucune	Centralised	Non	GPS, LTE, Bluetooth	Self-diagnosis
11 TerraHub Credential Link	Application	Private	None available	Hybrid: Mostly decentralised with centralised elements	Not	Blockchain	Both self diagnosis and validated diagnosis possible (depends on the credentials uploaded on the platform).

	Public health data	Limited Purpose	Limited retention	Security/Reliability	Jurisdiction (current and proposed scope)	Interoperability
	Yes	Limited to use in relation to COVID-19	Limited to retention in relation to COVID-19	Encryption Differential privacy Pseudonomization Security vulnerability for temporary GPS deployment	Current scope: Canada but potentially unlimited	Yes
	Depends on application (allegedly no)	Depends on application (allegedly limited to COVID-19)	Depends on application (allegedly limited to COVID-19)	Pseudonymization Encryption	First and only current deployment planned in France; scope potentially unlimited	Depends on application
	No	Limited to COVID-19 (further processing upon anonymization)	Limited to COVID-19 (further processing upon anonymization)	Pseudonymization Encryption	Germany (further rollouts are unlikely to happen)	None
	No	Limited to use in relation to COVID-19	Limited to retention in relation to COVID-19	Encryption Rolling Proximity Identifier	Subject to implementation	Likely but subject to implementation
	No	Limited to use in relation to COVID-19	Limited to COVID-19, capability for retention safeguards	Susceptible to BT-LE cyber hacking (eg wardriving). Uses rotatable ephemeral identfiers ("EphIDs")	Subject to national implementation	Likely but subject to implementation
	Allegedly no, but wide caveat built in	Allegedly single use but insufficient safeguards built in. High risk that it could easily be used for other purposes.	Allegedly limited safeguards on retention but insufficient safeguards built in.	Susceptible to BT-LE cyber hacking (eg wardriving). Uses rotatable ephemeral identfiers ("Sonar IDs")	Currently Isle of White but whole of UK proposed. Not outside the UK	No
	Yes	Limited to use in relation to COVID-19	Retained for 21 days on individuals' devices	Encryption Pseudonomization Non-personal identification information stored No access until consent	Singapore (but adopted by Australia through COVIDSafe) Accessible in U.S. and U.K. by holders of Singaporean phone number	Yes
	No	Limited to use in relation to COVID-19	Limited to retention in relation to COVID-19	Encryption	Cross-border scope	Yes
	Potentially yes	Limited to use in relation to COVID-19 and research	Limited to use in relation to OCVID-19 and research	Encryption, in some cases de-identification, and anonymization for research	Indeia	No
	No	The solution is fully programmable by each company that deploys it. There are no controls in place. High risk that it could easily be used for other purposes.	Nothing disclosed. Depends on each company that deploys the solution	Although data is said to be anonymised when transmitted to the backend, nothing has been disclosed regarding the security or reliability of the wearable device, the transmission of the data from the device to the backend, or the operation and storage of data on the backend.	Business is based in Poland (with offices in the US), but intends to distribute the solution world-wide	N/A
	Potentially yes	Initially deployed for workplace safety, extended to COVID-19 but not limited to it. Once the pandemic is under control, the features linked to COVID-19 are to be stopped.	Unlimited retention period for the information stored on-chain. Retention period for personal data stored off-chain will depend of the policy of such third-party database.	Encryption at-rest and in transit Privacy Enhancing Technologies QA/QC methods used	Current scope is Alberta, Canada but potentially unlimited	Yes

APPENDIX 3

PIA STUDY REPORTS

As part of the PostCoviData project conducted by the Human Technology Foundation, the summaries of the PIA Study Reports reproduced in this appendix have been prepared based on a review of publicly available documents by members of the ITechLaw Association who are cited as contributors to each of the respective documents. The contributors participated in this project in their personal capacities. Accordingly, the views expressed in the summaries of the PIA Study Reports do not reflect those of the law firms or other entities with which they may be affiliated. The contributors have worked diligently to ensure that the information contained in the PIA Study Reports is accurate at the time of publication. The publisher will be pleased to receive information that will assist in correcting any inadvertent errors or omissions.

- COVI-APP (MILA)
- DP-3T
- NHSX
- ROBERT
- CORONA-DATENSPENDE
- APPLE/GOOGLE
- TRACETOGETHER
- COALITION
- AAROGYA SETU
- ESTIMOTE
- TERRAHUB CREDENTIAL LINK

Montreal Institute of Learning Algorithms - MILA COVI Canada App PostCoviData Impact Assessment ("PIA")

June 1, 2020

ItechLaw Evaluation Committee
Charles Morgan, McCarthy Tétrault LLP
Manuel Morales, Université de Montréal
Allison Marchildon, Université de Sherbrooke

To be read in conjunction with Privacy Impact Assessment and whitepaper for COVI Canada App ("**COVI App**").

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

- COVI Canada App ("**COVI App**") is a decentralized contact tracing and risk assessment mobile application developed by a consortium led by the Montreal Institute of Learning Algorithms ("**MILA**").

- The application is designed to provide contact tracing among users, to assess their risk of COVID-19 infection and provide them with recommendations in relation to current behaviour or changes in risk level. It also aims at providing governmental authorities with aggregated information about contagion risks to assist them in designing more effective responses to the pandemic.

- Instead of providing a binary assessment (yes/no) of whether the individual has been in contact with another individual who has been diagnosed COVID-19, the AI/ML solution developed by MILA calculates the overall likelihood of users' exposure to COVID-19 (the "risk score"), based on demographic, health and behaviour information provided by the user, official diagnoses if available, and the risk scores of other users in the network. To the best of our knowledge, COVI is the only contact tracing app that is seeking to send multi-level risk messages.

- This solution allows copies of the application installed on users' devices to send and receive risk scores through a private messaging system. If official diagnoses become available, and a user tests positive as validated by public health authorities, other users who came into proximity with that user will be contacted through the private messaging system. The app will send a message that does not indicate time or place of contact informing these other users that they are at heightened risk and giving appropriate proposed courses of action, such as beginning to monitor symptoms.

- It prompts the user for a health status, pre-existing conditions and demographic parameters via an auto-diagnostics questionnaire. It then combines that information with GPS and bluetooth tracking to propose personalized non-binary recommended actions and tips. It uses a machine learning algorithm that predicts risk-based personalized actions to the user. It is also a platform to share confirmed positive COVID-19 diagnostics that would then propagate into the network of contacts to update the risk kevel and associated recommendations to all concerned users. Through the combination of GPS and Bluetooth handshakes, positive diagnostics and a machine learning algorithm it seeks to modify individual behavior to isolate (self-imposed confinement)

of high-risk individuals as new positive cases and their associated person-to-person contagion path emerges.

- The system utilises a hybrid decentralised of data storage and analysis. Most of the data is stored directly on the users' mobile devices. The information collected by the application will only be accessed by the MILA data trust in pseudonymous form in order to train and refine its machine learning-based risk assessment model, understand how widely the application has been adopted and how its features are being used, and determine whether the recommendations made are having an impact on a user's risk score. De-identified, aggregated data based on this information can be provided to government for epidemiological analysis and strategic planning. Geolocation data for contract tracing is exchanged through a private messaging system and protected from retracing by an encryption system.

- According to the COVI White Paper, "The pseudonymized data and geographical zone risk packets necessary for training predictive statistical and epidemiological models will be stored in a secured server with restricted access to selected AI researchers who will train these models. This machine will not be managed by the government; [MILA is] in the process of setting up COVI Canada, a not-for-profit organization focused on managing these data according to the highest standards of good governance and with the sole mandate to protect Canadians' health, well-being, dignity and privacy."

- The relevant data subjects will be individual citizens who have installed the COVI App (initially in Canada, primarily in Quebec).

- **The COVI App will process data on the basis of consent; its use will be voluntary.**

- Main regulatory requirements: Compliance with applicable privacy and data protections laws in the jurisdictions in which it is deployed. In Canada, these include *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("PIPEDA"); *An Act respecting the Protection of Personal Information in the Private Sector*, R.S.Q. 1993, c. P-39.1 ("**Quebec ARPPIPS**"), *Personal Information Protection Act* (British Columbia), S.B.C. 2003, c. 63 ("**BC PIPA**"); *Personal Information Protection Act* (Alberta), S.A. 2003, c. P-6.5 ("**Alberta PIPA**");

- Main ethical concerns: Privacy; Right not to be discriminated against; freedom of movement

- Although COVI App will be used to create a risk score for individuals, such information will not be used to make decisions about the individuals; rather it will be used (anonymously) to provide individuals with information that can help them reduce risks of harm for themselves and others

- Auditability is yet to be confirmed, but **the source code will be made open source** and publicly available for scrutiny.

- The impact of **COVI App data processing activity is significant** – it will enable citizens who have sufficiently uptodate smartphones to understand the risk of whether they have been in contact with other infected (or potentially infected) individuals and remove them from the chain of infection by means of **notifying them to self isolate and recommending actions to mitigate against risk, including self-isolation**.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

- Generally, use of the app is intended to help flatten the epidemiological curve of local COVID-19 epidemics and avoid new outbreaks by assisting with contact tracing, while protecting individual privacy.

- In particular, it is designed to be used on a voluntary basis and does not rely on tracing individual movement, but rather on proximity information regarding with respect to other users.

- The COVI App is designed to promote human agency and autonomy

- Users will have opportunities to provide express consent at several points during the data flow process, in order to control what information is collected and to whom it is disclosed.

- Moreover, the users can delete the app and their data at any given time (i.e. can remove their consent). Upon deletion, the algorithm is retrained and all data associated to a user is fully removed from the app and the aggregate data provided to public health authorities.

- Instead of providing a binary assessment (yes/no) of whether the individual has been in contact with another individual who has been diagnosed COVID-19, the AI/ML solution developed by MILA calculates the overall likelihood of users' exposure to COVID-19 (the "**risk score**"), based on demographic, health and behaviour information provided by the user, official diagnoses if available, and the risk scores of other users in the network.

- There is a concern that providing the risk score in numerical form could have negative consequences (e.g., creating panic in a user with a high score or providing an abusive partner with a "control point" to monitor the behaviour of their spouse). Instead, COVI App will provide information and recommendations in response to changes in the risk score. This approach intended to empower the user, putting them in a position to adopt the appropriate behaviours in response to their level of risk. Given that the

user's risk score is itself partially a function of the risk scores of other individuals, providing recommendations rather than a numerical score adds one further layer of obfuscation, thereby lowering the possibility of making inferences about the risk scores of other users.

PRINCIPLE 2 – ACCOUNTABILITY

- The pseudonymized data necessary for training predictive statistical and epidemiological models will be stored in a secured server with restricted access to selected AI researchers who will train these models.

- This machine will not be managed by the government; [MILA is] in the process of setting up a COVI Canada not-for-profit data trust specifically to manage these data."

- According to the COVI White Paper, "COVI Canada will have open rules about its governance, open access to the code and aggregated epidemiological models, and would be continuously monitored by its board, internal experts committees, and external evaluations from independent academic groups and governmental representatives, to make sure that it stays faithful to its mission. COVI Canada's entire governance model is built around the core values of legitimacy, accountability, transparency, and efficiency. [...] COVI Canada's single mission of supporting Canadians in their fight against COVID-19 and not-for-profit nature ensure the data collected will never be used for commercial purposes, nor sold to private companies. It cannot be used for surveillance or to enforce quarantine by governments. The data is all stored in Canada and will be deleted as soon as the pandemic is over."

PRINCIPLE 3 – TRANSPARENCY & EXPLAINABILITY

- Users will be all members of the general public without any heightened technical sophistication.

- According to the COVI Whitepaper, in order to help ensure key components of the terms and conditions are "well understood by users, not just agreed to haphazardly, [the terms are presented] using a multi-layered, progressive disclosure approach, which has been shown to balance user experience and system transparency. For example, a graphics-heavy top layer illustrating privacy implications can link to a somewhat more textual second-layer this can then link to the longer FAQ section on the website, which in turn sends users to the full privacy policy."

- According to the COVI Whitepaper, user comprehension is verified rather than assumed: "First, we apply in-app analytics to estimate users' comprehension for example, by looking at the average user dropout at various layers of disclosure information. Second, we administer dynamic comprehension quizzes to a random sample of users, allowing us to understand what information has and has not been internalized. Finally, disclosure tools are iteratively revised based on the feedback from these measures, to ensure they best cater to actual user behaviour."

- The output of the model can be explained and decisions can be audited. The user does not receive specific information as to how the risk assessment is calculated. The user will only receive personalized recommendations and tips that get updated as more information is available.

- Mila will make available a web page dedicated to this app (where the privacy policy will be available to app users), where it will explain how individuals may submit a complaint about Mila's handling of their personal information in relation to the app.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

- The data used will be a combination of user-reported and automatically generated data from the users devices. The extent to which the data will be "representative" will depend on the number of users and their relative demographic and geographic details. It is estimated that the contact tracing component of the COVI App will require an uptake rate of 60% of the general populace to ensure efficacy and accuracy. For the AI-aspect (aggregate data, epidemiological models, etc.),

MILA estimates that the minimal percentage of download required is much lower, namely approximately 10%.

- Marginalized groups are both the most likely to be affected and the least likely to be able to access and use a tool such as COVI. For this reason, MILA has indicated that the composition of the governance structure for the Covi Canada data trust will also be submitted to strong inclusion practices (i.e. representation of civil society, including vulnerable groups). Moreover, the algorithm will be trained to ensure the absence of biases and will be submitted to third party, independent algorithmic impact assessment, including on the front of diversity and inclusion.

PRINCIPLE 5 – SAFETY & RELIABILITY

- As a private messaging network that permits direct user input of demographic information, health conditions and symptoms, accuracy of risk assessment (and hence recommended actions to take) cannot be guaranteed if users enter false data about themselves. Risk scores propagated through the solution can be affected by such false entries but unless large numbers of users are dishonest (as a proportion of all users), mischief by individuals will not have significant effects.

- If a user receives an official diagnosis, a special token or one-time password will be given to the user by the health authority. In other words, such diagnoses will be validated by public health authorities and not self-reported.

- **Residual Risks:** Several premeditated attack scenarios have been identified by the developers as residual risks inherent to any automatic contact tracing system where account creation is unrestricted.

- Our view is that **these risks largely require a "tech savvy" and malicious bad actor**.

- The above points must be viewed in the context of use of the app by the general populace. Levels of technological sophistication must be assessed as low. Users will treat the app Tech Solution as they would any other app on their phone, however additional trust levels may be presumed as the app will be released with input and approvals from public health authorities. Expectations of safety, protection from harm and reliability of the Tech Solution will therefore be extremely high. Furthermore, it should be made absolutely clear that the App is not a medical device and (despite the notifications and recommendations) does not provide/is not a substitute for obtaining medical. As a result of all these considerations, **we are concerned at the potential for a mismatch in terms of actual safety and reliability levels and public expectations**.

- **Our recommendation is that a program of public awareness and education should be implemented** in a manner befitting of the wide spectrum of public consumption.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

- The solution has been designed to interoperate internationally.

- The solution will be made available subject to an open source license. The type of open source licensing model to be adopted has not yet been identified.

PRINCIPLE 7 - PRIVACY

- Privacy by design is built into the architecture of the COVI App

- Pseudonymized data will be transferred to the COVI Canada data trust for assessing risk score.

- According to the COVI White paper, in order to further improve user privacy, risk levels are quantized to 4 bits of precision before being exchanged.

- When a phone sends a message to another phone via the cryptographic servers, the receiver will not know from which phone (neither phone number nor IP address) the message comes from. To provide additional protection against stigmatization, these messages are sent with a random delay of up to a day.

- The information collected by the application will only be accessed by the COVI Canada data trust in pseudonymous form in order to train and refine its machine learning-based risk assessment model, understand how widely the application has been adopted and how its features are being used, and determine whether the recommendations made are having an impact on a user's risk score. De-identified, aggregated data based on this information can be provided to government for epidemiological analysis and strategic planning. Geolocation data for contract tracing is exchanged through a private messaging system and protected from retracing by an encryption system.

- Geolocation and timestamp data needed to provide the contact tracing function will be locally encrypted at rest on the device (as are all data collected by the application), hashed using a one-way hashing function immediately upon collection, and the original information will be discarded. Additional obfuscation methods will be deployed, either at launch or as rapidly as possible thereafter, to further limit the potential for opportunistic attempts to re-identify individuals from contact traces, whether by users of the system or by government actors.

- Much of the data collected is also deleted on an ongoing basis, namely :

  – Data in users' phones is deleted at the latest 30 days after its collection;

  – Data used to train the algorithm is deleted at the latest 90 days after its collection;

  – All data is deleted upon the declaration that the pandemic is over.

DP-3T Consortium
DP-3TPostCoviData Impact Assessment ("PIA")
Overarching Risk Summary (Key Findings)

May 9, 2020

ItechLaw Evaluation Committee
John Buyers, Osborne Clarke LLP
Trish Shaw, Beyond Reach
Nikhil Narendran, Trilegal
Lára Herborg Ólafsdóttir, Lex
Marco Galli, Gattai, Minoli, Agostinelli Partners Studio Legale
Rheia Khalaf, University of Montreal, Director Collaborative Research & Partnerships
Manuel Morales, University of Montreal, Associate Professor

To be read in conjunction with main PIA for DP-3T.

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

- DP-3T is a decentralised protocol for a contract tracing app hosted on Apple (iOS) and Google (Android) smartphoes which is designed to facilitate contact tracing in the general populace. It proposes an architecture which is capable of international deployment.

- The risk assessment for DP-3T (as a protocol) is contingent upon national implementations of the technology. As such the countries which take it up may have differing legal contexts and backgrounds, including in relation to general rules of law. As currently envisaged, DP-3T is primarily focussed on EU and European countries (including non-EU members such as the UK and Norway), all of which have mature democratic legal principles, established consistent data protection laws and laws preventing discrimination. Assessment of risks for countries outside this cohort is unquantifiable until further information on those countries' legislative and geopolitical contexts is provided.

- Data Protection (GDPR and associated legislation such as ePrivacy directive); laws applicable to the use of telecommunications networks; laws applicable to privacy, individual and mass surveillance will all be relevant to the use of DP-3T based apps.

- The main ethical concerns around the use of DP-3T based apps include Privacy, the Right not to be discriminated against, Freedom of Movement, Human Autonomy, Human Agency, Prevention from Harm, new kinds of discrimination associated with having the App or not having the App (not necessarily covered by existing equality laws), societal impact on trust (of provider and of co-users), and the right not to have an inference made about an individual or group of individuals

- DP-3T does not use AI or Machine Learning. Nevertheless, we do expect there to be a degree of Automated Decision Making in the roll-out of the national decentralised solution(s) which may invoke Article 22 of GDPR.

- The relevant Data Subjects will be individual citizens who have opted into use of the DP-3T app. Data types are pseudo randomised EphID BT LE (Bluetooth Low Energy) data packets generated by mobile phones. Data used could in very limited cases (particularly in the decentralised delinked operating model proposed in the DP-3T White Paper Design 1) be reconstituted pseudonomised data.

- Although the technological notification package of information sent when an individual is deemed infected itself contains no health data, the notification event could potentially be seen as health data or inferred health data, because only data

of COVID-19 positive persons, as confirmed by a healthcare professional, are uploaded to the backend server.

- DP-3T can be explained clearly – there is no issue of opacity in the solution as it is based on conventional BT LE communication between mobile phone handsets. Auditability is yet to be confirmed, but is based on open source code which is publicly available for scrutiny.

- The impact of DP-3T app data processing activity is significant – it will enable citizens to understand whether they have been in contact with other infected individuals and potentially remove them from the chain of infection by self isolation. In short, the processing will enable countries to better manage and mitigate the impact of their local COVID-19 epidemics

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

- DP-3T as conceptualised could be said to be compatible with the principles of human agency and autonomy as it is designed such that participation would be on a voluntary basis. However, this would depend upon the implementation at national levels.

- While the design of the DP-3T is compatible with the principles of human agency and autonomy, we recommend that the actual national rules of implementation should be created to foster human agency, autonomy and respect for fundamental rights. The current legislative framework applicable to the use of such apps is focussed predominantly on use of telecommunications devices which does not safeguard individual citizen use. In this regard we would refer the reader to the proposed draft Coronavirus Safeguards Bill, which has been suggested as a safeguarding measure in the UK.

- We would recommend imposing additional safeguards on data deletion. DP-3T proposal currently recommends that data are deleted from servers after 14 days, and the solution itself will "gracefully" and organically disassemble itself when no longer needed as users will stop uploading their data to the Authorisation server, or stop using it per se. Our proposal is that a "sunset" provision is added such that data are automatically deleted when an external agency (such as the WHO) declares the pandemic over.

- We would caution that contractually, any DP-3T based app will require to conform to both Apple's App Store standard agreement and Google's Play Store Agreement. Each of these agreements contain separate privacy related terms (Google Play store for example refers to Google's Privacy Policy, see section 9 of that Agreement; also see section 5.1 Apple's App Store Developer Agreement). These terms and conditions each has the ability to significantly affect (and potentially undermine) the privacy handling treatment of DP-3T.

- The general overarching risk of this app is that (like any other proximity/contact tracing application) it could be used for other purposes post-pandemic (ie for state surveillance purposes). The DP-3T consortium has been very careful (indeed assiduous) to prevent this risk materialising for DP-3T, in particular significant design steps in the architecture DP-3T have been taken to maintain a decentralised structure, and to minimise instances in the design where personal data are used or may be inferred.

- There are undoubted public benefits to the use of apps such as DP-3T. Use of the app will potentially allow nation states to flatten the epidemiological curve of local COVID-19 epidemics. It may be that granular contact tracing and observation generally improves the science of epidemiology. This information could aid scientists in learning the proximity graph surrounding an infected user by providing details of their interaction with other persons and any consequent spread of infection.

- We remain concerned at the potential for such technological solutions to drive undesired "herd" behaviours in society – leading to automation bias (unconditional trust in outcomes driven by the app), driving false confidence at one extreme and ostracization of individuals at another. Such behaviours may most obviously be directed to infected individuals but may also be extended to those individuals who do not possess a smart phone and are therefore "disenfranchised".

PRINCIPLE 2 – ACCOUNTABILITY

- As noted above, the risk assessment for DP-3T (as a protocol) is contingent upon national implementations of the technology, which have the potential to significantly impact any wider risk assessment of the solution (for example by imposing mandatory installs or mandatory quarantines following a Covd-19 positive notification). We are unable to make definitive suggestions in the absence of such national implementations, but have made summary observations based on our current knowledge which may impact upon such implementations.

- We would recommend that the DP-3T consortium publish a framework of standard national rules and guidelines to which use of DP-3T is subject, this

can serve as guidance to governments to ensure international co-operation, consistency of national use and application and maximise interoperability between countries. Such national standard rules should provide for individual citizens to rectify identified errors in their data held on the "backend" DP-3T server.

- Third party dependencies also have the potential to significantly undermine accountability in the solution. In this regard we would identify the major OS platform providers, Apple and Google. Our recommendation in this regard is that these vendors be required to undertake separate and publicly available DPIA assessments and provide mandatory undertakings (or similar enforceable commitment) to conform to national rules specific to COVID-19 pandemic tracing. Such undertakings will require not only conformity with national rules based frameworks but also transparency to enable minimisation (and correction) of cross-platform errors in their technological solutions.

PRINCIPLE 3 – TRANSPARENCY & EXPLAINABILITY

- We are satisfied that Operation of the system in terms of data classes and functionality is clearly set out in the White Paper and accompanying documentation. The Backend and Authorisation servers should be fully auditable, subject to access being provided by local implementing authorities. We observe that this is not a centralised system – it is highly distributed. Local data held on smartphones will be outside scope of inspection and audit unless access is granted by (or court orders are sought effecting same).

- The DP-3T system is susceptible to Bluetooth LE and other cyber risks specific to this technology. These risks are not unique to DP-3T but are generic to distributed solutions of this nature. We detail some of these risks below, in the context of Principle 5 (Safety & Reliability) below. In our opinion, there is little information in the documentation to suggest robustness in DP-3T above and beyond any other BT LE enabled system.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

- As noted above, the risk assessment for DP-3T (as a protocol) is contingent upon national implementations of the technology, which have the potential to significantly impact any wider risk assessment of the solution (for example by imposing mandatory installs or mandatory quarantines following a Covd-19 positive notification). We are unable to make definitive suggestions in the absence of such national implementations, but have made summary observations based on our current knowledge which may impact upon such implementations.

- DP-3T is designed such that participation would be on a voluntary basis. We are concerned however that a segment of national populations (roughly 40% of over 65 year olds, and under 16s) may be excluded from participation simply because they do not have access to or own a smart device.

- We have already indicated that the DP-3T app (in common with similar solutions) could drive undesired "herd" behaviours in society – leading to automation bias (unconditional trust in outcomes driven by the app), driving false confidence at one extreme and ostracization of individuals at another.

- We are of the view that there needs to be an established system of redress for false positives and false negatives, as well as re-identification risks, co-locations risks, and proxies. As we have suggested under Principle 2, above, we would recommend that the DP-3T consortium publish a framework of standard national rules and guidelines to which use of DP-3T is subject, this can serve as guidance to governments to ensure international co-operation, consistency of national use and application and maximise interoperability between countries. Such national standard rules should provide for individual citizens to rectify identified errors in their data held on the "backend" DP-3T server.

PRINCIPLE 5 – SAFETY & RELIABILITY

- All proximity tracing systems that notify users that they are at risk enable a motivated adversary to identify the infected person (whether that be through multiple accounts, manual logging and/or logging/identifying epochs (time intervals) coupled with photo/video identification). Coupled with this, Bluetooth Low Energy has inherent weaknesses which are capable of exploitation with varying degrees of sophistication, such as noise injection, tracking of users using aspects orthogonal to contact tracing (ie. by logging MAC addresses), wardriving, and theft of mobile phones.

- Our view is that these risks largely require a "tech savvy" and malicious bad actor. The DP-3T protocol has sought to be as privacy preserving as possible and to minimize the risks of re-identification as much as possible (especially in Design protocol 2). As noted under Principle 3 above, there is little information in the documentation to suggest robustness in DP-3T above and beyond any other BT LE enabled system.

- The above two points must be viewed in the context of use of the app by the general populace. Levels of technological sophistication must be assessed as low. Users will treat the app Tech Solution as they would any other app on their phone, however additional trust levels may be presumed or required (dependent on culture) as the app will be released by national health authorities (and/or governments). Expectations of safety, protection from harm and reliability of the Tech Solution will be high. We are concerned at the potential for a mismatch in terms of actual safety and reliability levels and public expectations.

- Our recommendation is that a program of public awareness and education should be implemented in relation to each national implementation of DP-3T. In this regard, an explanatory "comic" is available in many languages on another GitHub webpage made available by the DP-3T consortium to assist public engagement.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

- As we have noted above, DP-3T has been released on an open source basis. Data classes are compact ephemeral IDs which are capable of being transmitted via BT LE protocols. Full publication has taken place of system architecture to enable this portability. Given the need to assess actual national implementations of DP-3T, we are unable to review actual interoperability standards.

- We understand from the separate DPIA that location data may be processed for the sole purpose of "allowing the application to interact with similar applications in other countries". It is unclear if this refers to country-specific implementations of the system or to other decentralized tracing control applications. Further technical evaluation would be required to assess this capability, and additionally to understand the extent to which data could be shared as between centralised and de-centralised tracing apps.

- So far as wider data sharing are concerned, the DP-3T protocol does not, for privacy reasons, currently envisage the sharing of proximity graphs with epidemiologists, although we note that this functionality may be enabled in later versions.

- The open source nature of the DP-3T solution is confirmed by the fact that it is licensed under the MPL 2.0 open source license framework. MPL 2.0 is a simple copyleft license which encourage contributors to share modifications they make to the code, while still allowing them to combine their own code with code under other licenses (open or proprietary) with minimal restrictions. Given this context, we do not anticipate complex intellectual property risk issues, although we must flag the protocol's dependence upon proprietary technologies such as Apple's iOS and Google's Android operating system. To a lesser degree we would also indicate that BT LE is itself a patented technology.

PRINCIPLE 7 - PRIVACY

- Our recommendations are consistent with the separate DPIA evaluation conducted by the EPFL (Prof. Eduouard Bugnion) and id est avocats Sàrl (Michel Jaccard and Alexandre Jotterand), Version 1.0, published 1st May 2020.

- In general, we consider that personal data may be processed as part of the system in limited cases. Even in the delinked model (see model 2 specified in the White Paper), it may be possible to use indirect means to correlate and confirm personal data elements to the extent necessary to identify indivduals, and this will certainly be the case where consent is obtained to upload data relating to infected individuals onto a backend server. Even if, in most cases, the ECJ ***Breyer*** test cannot be satisfied, we are fully in agreement with the DPIA authors that a conservative approach must be taken and the solution treated as if it is processing personal data.

- In the context of the second point under principle 7, we also find that such personal data may also contain potentially sensitive data (such as health data). Even though the technological notification package of information sent when an individual is deemed infected itself contains no health data, the notification event itself could potentially be seen as health data or inferred health data, because, only data of COVID-19 positive persons, as confirmed by a healthcare professional, are uploaded to the backend server.

UK: NHSx COVID19 App
NHSx COVID19 App: PostCoviData Impact Assessment ("PIA") Overarching Risk Summary (Key Findings)

May 16, 2020

ItechLaw Evaluation Committee
John Buyers, Osborne Clarke LLP
Patricia Shaw, Beyond Reach Consulting Limited

To be read in conjunction with main PIA for NHSx COVID19 App ("**NHSx App**").

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

- As at the time of writing this report, the NHSx App is **currently in beta testing** in the Isle of Wight (a little island off the south coast of England which is a part of the British Isles). The NHSx App utilises a centralised model (as opposed to a decentralised model) for proximity tracing – see diagram below. It is based on conventional BT LE communication between mobile phone handsets. Its goal is to simplify and accelerate the process of identifying the people who have been in contact with a person who has been tested positive with SARS-CoV-2 virus.

- The NHSx App is **reliant on the user's self-diagnosis (which may be confirmed or unconfirmed**). It utilises information about proximity encounters (the Transmitted IDs, i.e. encrypted Sonar ID, together with a timestamp for the encounter, and radio signal strength indicator information) uploaded by users either when they have either (a) "self-diagnosed" as infected (based on their presentation of symptoms assessed in the tool) OR (b) they report that they have confirmed results that they tested positive for the virus. The information provided should reveal to the centralised backend Sonar server the devices that were in close promity to one another, the duration and the distance of that proximity.

- As part of the self-diagnosis journey, the App includes a facility for a user to request a unique one-time use Reference Number from the Sonar Backend. When requested this is then presented to the user via the App. This is a unique identifier that can be used to request a test for COVID-19 and to **interface with human operatives** at a purposed call centre.

- The system utilises **a centralised model run by a governmental authority** which has expressed an appetite for future versions of the App to give users the functionality to donate data for further research. Therefore there is a **greater risk** of:

  – feature/mission creep;

  – utlising information in a way that may not be technically unlawful but could be seen as privacy invasive, such as monitoring of social interaction/contact graphs;

  – information directly obtained through the NHSx App being linked with other data records either held diirectly by or indirectly accessible to the governmental authority (such as National Central Healthcare Record, geolocation data records from mobile phone providers, information from third party API/operating providers, etc) resulting in the data being easier to re-identify;

  - new kinds of discrimination/sigmatisation forming due to pressure from those in Authority/ Civic Leaders to conform/fulfil "civic duty" (e.g.requiring download of App before returning to work); and

  - cyber attacks as a centralised database is likelt to be seen as a "honey pot".

- Although the UK government must comply with existing laws to protect Human Rights, protect personal data and prevent discrimination (amongst other laws applicable to the use of telecommunications networks; privacy, individual and mass surveillance), it has been highlighted amongst both legal practitioners and academics that **there is need for additional laws**. It is proposed that additional law provide appropriate safeguards and/or management of possible systems misuse from malicious actors, mission creep and to prevent new forms of discrimination occuring (to the degree not already covered by GDPR, e-Privacy Directive, Equality Act, Digital Economy Act 2017, Computer Misuse Act,of the Investigatory Powers Act 2016. For example, – it is unclear to what degree the Part 3, section 61A of the Investigatory Powers Act 2016 (which enables people with symptoms or a diagnosis of Coronavirus to be tracked without notice), will enable such investigatory authorities to have access to information either in transit or in storage. To this end, we note the draft Coronavirus (Safeguards) Bill.

- Its proposed architecture is said not to be compatible with forthcoming Apple (iOS) and Google (Android) Application Programming Interface, and therefore may have **particular problems when deployed on Apple smartphones**. Because of its centralised architecture, the NHSx App is **unlikely to be capable of international deployment and does not currently demonstrate that it is interoperable** with other protocols. such as DP-3T..

- Due to the privacy concerns and possible technological issues relating to "always on" BT LE capability, **a parallel development has commenced** utilising the decentralised architecture proposed by Apple and Google.

- This **Key Findings report is based on the current centralised beta version of the NHSx App** and not the parallel development whose details have not yet been disclosed.

- The relevant data subjects will be individual citizens who have installed the NHSx App, but at present the **NHSx App does not process data on the basis of consent, but instead relies on other lawful bases for processing**.

- The **NHSx App is using automated decisioning** (and therefore it invokes Article 22 of GDPR), but is not using consent as the lawful basis on which to conduct such automated decisioning. Although the NHSx App does not use other significant AI or Machine Learning, it is likely that the centralised backend Sonar server will (further details have not been disclosed).

- PECR/e-Privacy Directive is also likely to apply in respect of cookies or similar technologies, but mention of it is omitted from the Trial Privacy Policy. (NB: Regulation 6 of PECR would ordinarily require consent as the basis for processing cookies or similar technologies, unless an exemption, such as "the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network" applied.

- See Box 1 below for the lawful bases on which NHSx App appear to be processing data.

Lawful Processing Bases

ACCORDING TO THE TRIAL PRIVACY POLICY

Department for Health and Social Care's legal basis for processing your personal data under the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018 legislation is:

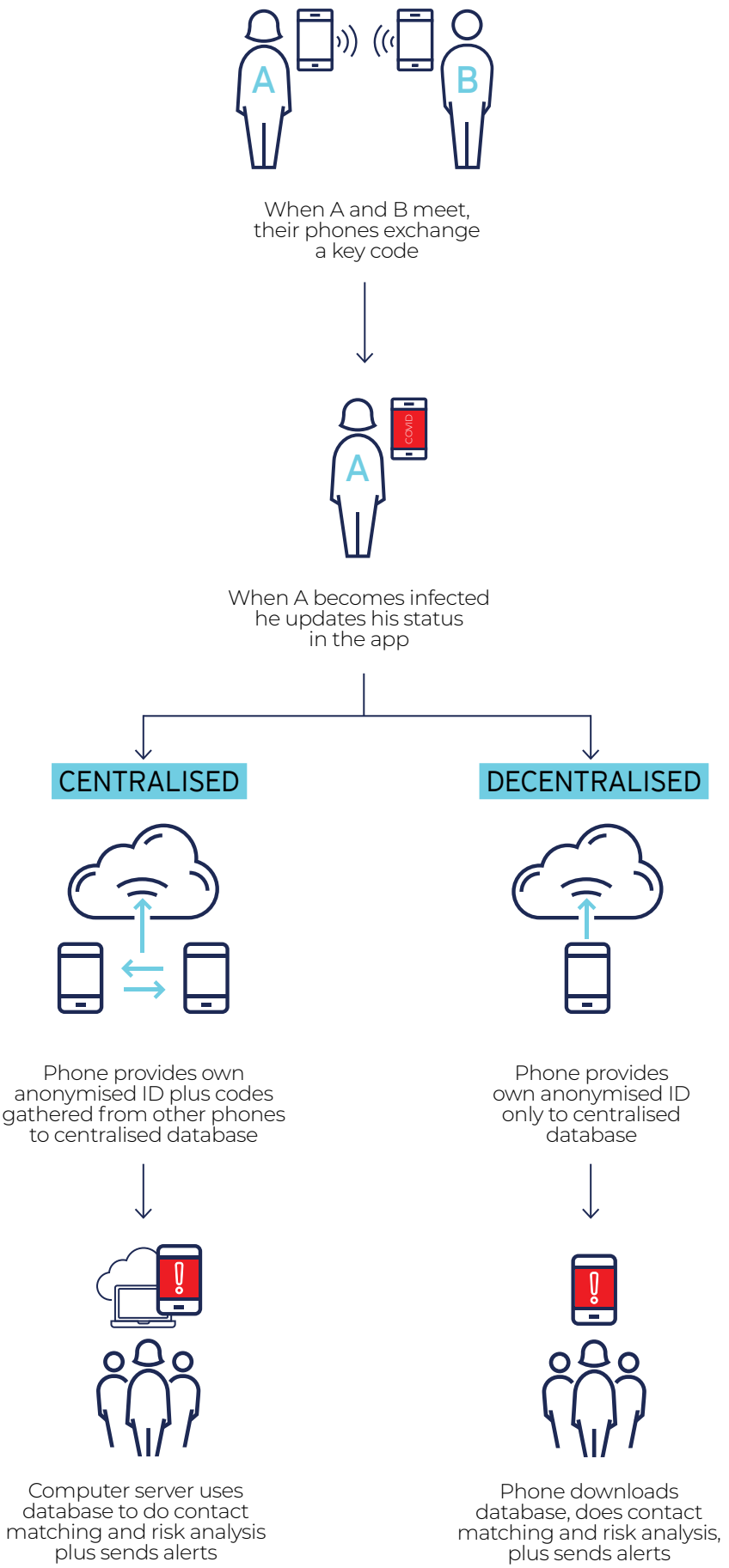
- GDPR Article 6(1)(e) – the processing is necessary for the performance of its official tasks carried out in the public interest in providing and managing a health service
- GDPR Article 9(2)(h) – the processing is necessary for medical diagnosis, the provision of health treatment and management of a health and social care system
- GDPR Article 9(2)(i) – the processing is necessary for reasons of public interest in the area of public health
- DPA 2018 – Schedule 1, Part 1, (2) (2) (f) – Health or social care purposes

The other organisations involved in processing your data, as set out in this Notice will be doing so either with an agreement in place with DHSC to provide that service, or with a legal basis of their own."

IN THE DPIA IT ALSO STATES

For provision of public health exception is underpinned by Regulation 3 of the Health Service (*Control of Patient Information Regulations*) 2002.

- Although the technological notification package of information sent when an individual is deemed infected itself contains no health data, **the notification event could potentially be seen as health data** or inferred health data, because only data of COVID-19 positive or suspected positive persons are uploaded to the backend server.
- The NHSx has not followed the most transparent process nor has it been readily forthcoming with detailed information about the App. Unfortunately for a long time much information in the public domain was conflicting and damaging to trust. **A DPIA has been produced for the Isle of Wight trial, but was first published after the trial had already commenced. We have not seen any further DPIA for a UK wide rollout. We would expect one to be published as a matter of short order.**
- **There should be an independent body** (as recommended by the UK Parliament's Joint Committee on Human Rights) to oversee the use, effectiveness and privacy protections of the app and any data associated with this contact tracing. The independent monitoring body should have, at a minimum, similar enforcement powers to the Information Commissioner, to oversee how the app is working. It must also be able to receive individual complaints. The monitoring body must be given sufficient resources to carry out their functions. The DPIA notes an independent **Ethics Advisory Board was constituted** to obtain views on the proposed processing activities (although it is unclear to what extent their remit can affect NHSx decision making), and further consultations were carried out with the National Data Guardian's Panel and the Centre for Data Ethics and Innovation. **As a minimum we would recommend that any continuing oversight be drawn from the same panel of experts.**
- Auditability is yet to be confirmed, but is based on open source code which is publicly available for scrutiny.
- The impact of **NHSx App data processing activity is significant** – it will enable citizens who have sufficiently uptodate smartphones to understand whether they have been in contact with other infected (or potentially infected) individuals and remove them from the chain of infection by means of notifying them to self isolate and **recommending that those that they live with also self-isolate**. In short, the processing has an impact on an individual's (and those that they live with) freedom of movement and autonomy. The NHSx App should enable the UK (if used amongst other measures) to better manage and mitigate the impact of their local Covid-19 epidemic in part. What is clear is that it is and cannot be the entire solution to the current pandemic.


A
B
When A and B meet, their phones exchange a key code
A
COVID
When A becomes infected he updates his status in the app
CENTRALISED
DECENTRALISED
Phone provides own anonymised ID plus codes gathered from other phones to centralised database
Phone provides own anonymised ID only to centralised database
Computer server uses database to do contact matching and risk analysis plus sends alerts
Phone downloads database, does contact matching and risk analysis, plus sends alerts

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

- Contractually, NHSx App will be required to conform to both Apple's App Store standard agreement and Google's Play Store Agreement. Each of these agreements contain separate privacy related terms. Full commentary of these agreements is out of scope of this review but each has the ability to significantly affect the privacy handling treatment of NHSx App. The Operating System Providers (Apple and Google) learn that the User installed the User App and has registered for the push notification service, but cannot see any data. Nevertheless, since they provide the operating system running on mobile devices, one has to trust them, since they could potentially learn information related to the proximity tracing system (who is infected, who infected whom, social graphs, etc.) and that this is a common factor to all CT Apps such as and including NHSx App.

- The NHSx App being a centralised and a governmental deployment model highlights further the importance of transparency, the purpose being limited, data collection and storage being minimised and kept secure.

- It appears that the individual's response to the notification is voluntary, and there a degree of human autonomy is maintained. Messaging has to be less emotive and coercive than "Support our NHS" "Save lives" "do your civic duty for the benefit of all in society" "play your part in the fight against coronavirus"

- Original intended aim is good, but here is a significant risk of function creep and/or for mass surveillance to ensue. We would recommend that; **demonstrating transparency, accountability and that they are seeking to be privacy preserving and ethical in the way that the NHSx App is made available and continued to be deployed is paramount, as is the creation of independent oversight**.

- There are some of the risks we associated with what the NHSx App of what it could potentially do for us as a society and what it could potentially do to us as a society.

- Potential promise of Health benefit/reduction in cases of COVID19.

- Our smart devices are to become a Proxy for human beings and their relationships.

- Potential to affirm or undermine trust in Government, NHS, other citizens.

- Potential to provide a false sense of confidence or reassurance by having a technological solution that is one part of a wider strategy.

· Any other risks (such as for example, the identification and potential singling out of infected individuals and/or those that are required to self-isolate) and the general increase in levels of anxiety of the general public about the virus and leaving one's home / circulating amongst people would be generic to all other contact tracing apps and need to be balanced carefully against the undoubted positive impact to society (and human health) in the use of such technology.

· There is **indecision in the UK as to whether to adopt a centralised or decentralised app**. Lack of ubiquity (ie more than one app being used by the general populace) will potentially reduce the efficiency of all apps in use and increase general confusion in the populace. It also creates additional complexity in relation to potential interoperability issues.

· The current DPIA for the Isle of Wight Trial is inherently contradictory as to how user data is handled (in the context of the centralised app) and this has been heavily criticised by privacy campaigners and academics. Although you can delete data from your handset, it is apparent that this will not necessarily lead to data being deleted from the Sonar central server.

OUR RECOMMENDATION WOULD BE:

- **To implement legislation to provide additional safeguards, including redress, (such as that proposed by the Coronavirus Safeguards Bill) help build trust and mitigate against risks of failure outlined in the PIA.**
- To have a plan to protect those who are digitally excluded and do not have access to or own a smart device should be put in place, both to protect those not included (likely ageing, vulnerable, young children, healthcare needs and mental capacity issues) but also as a strategic fallback if the NHSx App fails to function or scale as intended. We note that the NHSx is considering the DevicesDotNow initiative.
- **To ensure that appropriate safeguards are put in place regarding the recommendations and notifications to ensure that they are proportionate and appropriate to the end user** (i.e., messaging must be right for child recipient vs adult recipient of notifications. Vulnerability of the user will determine how likely that individual is to comply with recommendations or not, and/or what they do with that information (n.b.: risk of suicide and/or other mental health issues).
- Safeguards for all should include, **clarity over what happens to ALL data after App is deleted and under what circumstances an individual's right to access the NHS App might be ended by NHS.**

PRINCIPLE 2 – ACCOUNTABILITY

- NHSx is a health authority sat under the governmental Department of Health and Social Care. **It should be held accountable like any other government or public authority**, in particular in respect of Human Rights and Equality Act violations.

- The NHS to which NHSx forms a part is a long standing health authority which should have organisational and accountability constructs already established. That said, it is not experienced in the deployment and ongoing governance and oversight of proximity tracing tools. Although it has established an Ethics Advisory Board which provides advise to the (presumably internal to NHSx) App Oversight Board (see EAB Terms of Reference here), it is not clear what role or decision making power the App Oversight Board has. **Our recommendation is that independent oversight be established.**

- It was not clear what (if any) training NHSx would either receive or conduct internally to ensure it had sufficient capability in the event of a change of service provider.

- As a public health authority and not a technological solutions provider it is highly likely that NHSx will rely heavily on the experience of its consortium of technological services providers. These include Amazon Web Services (AWS), Pivotal/VMWare Tanzu and Microsoft Azure. It is unclear from the DPIA or the Press claims what role (if any) Palantir plays within the consortium, but may be assisting with understanding the anonymised data. All are experienced technology developers. **Our recommendation would be for NHSx to build capacity in this regard.**

- Most significantly (and this is likely to be as a result of the current legal processing basis position taken in the DPIA see summary and Box 1 above) **there are insufficient access and rectification safeguards built into the NHSx App model**.

- Third party dependencies also have the potential to significantly undermine accountability in the solution. In this regard we would identify the major OS platform providers, Apple and Google. **Our recommendation in this regard is that these vendors be required to undertake separate and publicly available DPIA assessments and provide mandatory and legally enforceable undertakings in relation to their treatment of NHS App data, including metadata derived from user behaviour. Such undertakings will require not only conformity with UK law, regulations and NHSx Codes of Conduct but also transparency to enable minimisation (and correction) of cross-platform errors in their technological solutions.**

PRINCIPLE 3 – TRANSPARENCY & EXPLAINABILITY

- As noted above, the NHSx App is in beta testing on the Isle of Wight as a pilot project to assess the robustness of the centralised app model. As part of that pilot, Terms of Use, a Privacy Policy and a DPIA have been published. However the results of the Isle of Wight trial have not yet been published and therefore there is no conclusive position. We also await the documents for the full implementation of the NHSx App for the wider UK

- That said, the functionality of the app and data classes used are explainable.

- The NHSx App is susceptible to Bluetooth LE and other cyber risks specific to this technology. These risks are not unique to a centralised proximity tracing tool, but are generic to solutions of this nature. We detail some of these risks below, in the context of Principle 5 (Safety & Reliability) below. In our opinion, there is little information in the documentation to suggest robustness in NHSx App above and beyond any other BT LE enabled system.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

- The DPIA for the IOW trial states that Art 22 of GDPR applies but that the **grounds on which they are relying on are not consent**. It would appear that they are relying on Regulations 3(1) and 3(3) of the Health Service (Control of Patient Information) Regulations 2002 as the exception which "lays down suitable measures to safeguard the data subjects rights and freedoms and legitimate interests. See Michael Veale's DPIA legal analysis for reasons as to why this exception might not apply to automated decision making.

- Irrespective of whether ADM applies or not, because of the nature of the App and the notification service it provides, individuals are likely to be influenced by automation bias when accepting the recommendations of the app. Furthermore, the following additional qualifiers are important to note which could have a significant impact on fairness or non-discrimination, that is:

  – the content of the notifications,

  – the sanctions (if any) for non-compliance with such notifications (including but not limited to legal sanctions but also those related to return to work, particularly after a period furlough), and

  – the limitations compliance/non-compliance pose (e.g. financial constraints/socio-economic circumstances)..

- NHSx App is designed such that participation would be on a voluntary basis. We are concerned however that a **segment of national populations (roughly 40% of over 65 year olds, and under 16s) may be excluded from participation simply because they do not have access to or own a smart device**.

- We have already indicated that the NHSx App (in common with similar solutions) could **drive undesired "herd" behaviours in society** – leading to automation bias (unconditional trust in outcomes driven by the app), driving false confidence at one extreme and ostracization of individuals at another.

- We are of the view that there **needs to be an established system of redress** for false positives and false negatives, as well as re-identification risks, co-locations risks, and proxies.

- By virtue of the fact that the NHSx App uses a centralised server it is likely that **users travelling across different Member States cannot be efficiently notified. A big risk for border towns between Northern Ireland and the Republic of Ireland**. The fact that the NHSx App is currently not interoperable with other EU solutions, could be a cause of discrimination or unfairness for cross border workers/families.

- In light of the above considerations, there is a risk of new kinds of discrimination occur by virtue of having/not having the NHSx App.

PRINCIPLE 5 – SAFETY & RELIABILITY

- **All proximity tracing systems that notify users that they are at risk enable a motivated adversary to identify the infected person** (whether that be through multiple accounts, manual logging and/or logging/identifying epochs (time intervals) coupled with photo/video identification). Coupled with this, BT LE has inherent weaknesses which are capable of exploitation with varying degrees of sophistication, such as noise injection, tracking of users using aspects orthogonal to contact tracing (ie. by logging MAC addresses), wardriving, and theft of mobile phones.

- Our view is that **these risks largely require a "tech savvy" and malicious bad actor**. As noted under Principle 3 above, there is little information in the documentation to suggest robustness in NHSx App above and beyond any other BT LE enabled system.

- Contractually, in respect of the Isle of Wight Trial, the NHSx App has sought to mitigate against some of the malicious circumstances in and through its Terms of Use.

- The above points must be viewed in the context of use of the app by the general populace. Levels of technological sophistication must be assessed as low. Users will treat the app Tech Solution as they would any other app on their phone, however additional trust levels may be presumed as the app will be released by the UK's governmental Department of Health and Social Care under the auspices of NHSx health authority. Expectations of safety, protection from harm and reliability of the Tech Solution will therefore be extremely high. Furthermore, it should be made absolutely clear that the App is not a medical device and (despite the notifications and recommendations) does not provide/is not a substitute for obtaining medical. As a result of all these considerations, **we are concerned at the potential for a mismatch in terms of actual safety and reliability levels and public expectations**.

- **Our recommendation is that a programme of public awareness and education should be implemented** in a manner befitting of the wide spectrum of public consumption. The UK might want to take their lead from the DP3T consortium's proposal of an explanatory "comic" to assist public engagement .

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

- NHSx App in beta testing phase has been released on **an open source basis under the permissive** MIT Licence open source licence. Given this context, we do not anticipate complex intellectual property risk issues, although we must flag that that my change with any dependence upon proprietary technologies such as Apple's iOS and Google's Android operating system. To a lesser degree we would also indicate that BT LE is itself a patented technology.

- The NHSx App is designed for UK use only. Insufficient information has been disclosed to review actual interoperability standards, but given it is based on a centralised approach and is currently not compatible with the proposed Google and Apple API, it is unlikely to be interoperable.

- As stands under the Isle of Wight trial,

  – any data sharing that is envisaged with service providers is apparently under GDPR compliant contracts. It is not fully clear where cloud servers are based and therefore where data might be hosted (as some are specified as west Europe and/or default server).

  – Data will be shared with NHS England and NHS Improvement under existing processing powers pursuant to the notice issued by the Secretary of State under s. 3(4) of the Health Service (Control of Patient Information) Regulations 2002.

  – Purposes for which data will be obtained, include: data analysis for public health planning and pandemic response, such as resource planning and epidemiological modelling; and using de-identified or anonymised data for scientific research and statistical analysis

PRINCIPLE 7 - PRIVACY

- In general, **we consider that personal data may be processed as part of the system . It may be possible to use indirect means to correlate and confirm personal data elements to the extent necessary to identify indivduals**, and this will certainly be the case where consent is obtained to upload data relating to infected individuals the central Sonar server. Even if, in most cases, the ECJ ***Breyer*** test cannot be satisfied, we are fully in agreement that a conservative approach must be taken and the solution treated as if it is processing personal data.

- We also find that such personal data **may also contain potentially sensitive data (such as health data)**. Even though the technological notification package of information sent when an individual declaring themselves as infected itself contains no health data, the notification event itself could potentially be seen as health data or inferred health data, because, only data of COVID-19 positive (or suspected) persons are uploaded to the central Sonar server.

- See Principle 4 and the Factors Justifying Impact Assessment above regarding lawful basis used for processing personal data during the Pilot.

INRIA and Fraunhofer AISEC ROBERT Protocol PostCoviData Impact Assessment ("PIA") Overarching Risk Summary (Key Findings)

May 15, 2020

by Alexander Tribess (Weitnauer Partnerschaft mbB, Germany)
Edoardo Bardelli (Gattai, Minoli, Agostinelli and Partners, Italy)
Licia Garotti (Gattai, Minoli, Agostinelli and Partners, Italy)
Doron Goldstein (Katten Muchin Rosenman LLP, United States)
Dean Harvey (Perkins Coie LLP, United States)
Jenna Karabil (Law Office of Jenna F Karadbil, P.C., United States)
Smriti Parsheera (CyberBRICS Project, India)

To be read in conjunction with main PIA for the ROBERT protocol, dated 10 May 2020.

The ROBERT (ROBust and privacy-presERving proximity Tracing) protocol is a proposal for the Pan European Privacy-Preserving Proximity Tracing (PEPP-PT) initiative, whose main goal is to enable the development of contact tracing solutions respectful to the European standards in data protection, privacy and security, within a global response to the pandemic. Therefore, any risks would largely be with the implementing apps. However, many of these risks are inherent with a centralized server system.

It has to be noted that, for the time being, "StopCOVID", supported by the French government, appears to be the only application built on the ROBERT protocol. It has been reported that many other countries that were said to be backing PEPP-PT have now moved to DP-3T, using a de-centralized structure instead of the centralized ROBERT approach. Some of the initial developers of the PEPPP-PT are also reported to have abandoned the project due to centralization, transparency and privacy concerns.

The objective of applications such as "StopCOVID" – and the ROBERT protocol behind them – is to trace contacts of a certain proximity and duration between citizens. Once a user gets positively tested on COVID-19, and shares this information with the application (i.e. health data), the application would warn other users that were in close contact with the infected person during the infectious period. To detect whether two users have been in proximity to each other, the applications rely on short-range communications exchanged using the Bluetooth wireless technology activated on both users' devices. Thus, the application could help facilitate and accelerate the spread of information amongst citizens concerning possible infections.

One of the ideas behind the PEPP-PT initiative was to develop a protocol that could serve as a basis for various "national" apps which would then be able to interact with each other. Especially within the European single-market and the Schengen area, cross-border travel is likely to increase significantly once travel restrictions have been withdrawn. Therefore, it is likely that applications based on the ROBERT protocol will be used for cross-border travel and, thus, in different jurisdictions.

As applications based on the ROBERT protocol would be processing personal data of users, the main regulatory requirements would be laws on privacy and data protection (such as the GDPR for EU/EEA member states, or national laws on data protection, e.g. in Switzerland). The main ethical concerns are that (a) a centralised system could be more amenable to mission creep by the governments ; (b) people could be stigmatized if, by using the application, it would become publicly known that they had been infected with COVID-19 and spread the disease ; (c) from the data collected through the application, malicious users and/or organizations could draw contact and/or movement profiles of a large number of people.

As regards the stakeholders, apart from the developers of ROBERT itself, a couple of other stakeholders

need to be considered: There will be developers of the applications based on the ROBERT protocol. It is likely that applications would be provided by government agencies (e.g. national health agencies) ; however private initiatives are not excluded from using the protocol. As the ROBERT protocol suggests a centralized model, there must be a provider for the central server (perhaps a national health agency if run by a government).

The ROBERT developers team puts a strong emphasis on the fact that data would be transmitted pseudonymously. In addition, due to the centralized server model, the protocol does only collect very little information on the concrete circumstances of a contact. With a centralized approach, the calculation of the risk of contagion is done on the server side, without taking into account the quality of contacts nor personal information. The result could, therefore, be unreliable, with probably many false positives as opposed to a de-centralized approach where much more information may be collected and stored on the user's device. In terms of explainability, the results (i.e. the warning messages sent to users) cannot be explained to the specific user because the user will not get any information on the location or exact time of the contact ; the user must trust the application without being able to gather any further information as regards the "real" risks.

Data will be processed on a very large scale. It is the idea behind any contact tracing solutions that as many people as possible have respective applications on their mobile devices and keep them activated. If applications were actually used by a very large number of people in a given populations (maybe 60 % or more), contact tracing applications are said to become an important instrument to contain the virus.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

ROBERT could provide the deployer – being it national or private (i.e. a research institute) – with a better understanding of the spreading of the pandemic and – potentially – it may contribute in flattening the epidemiological curve.

However, the technology itself, and especially the risks that are inherent to the centralized structure, also bear the risk that data collected through applications could be processed for other purposes than mitigating the COVID-19 pandemic by tracing contacts. The more contact information is transmitted to the server, even if this information is pseudonymized/anonymized, the greater the risk of attacks. The more information the central server stores, the greater the risk of loss of anonymity and confidentiality, as the success of cryptanalysis attacks increases with the amounts of encrypted samples available.

It must be noted, also from an ethical perspective, that the ROBERT protocol is published under an OpenSource software license (MPL 2.0, https://www.inria.fr/fr/contact-tracing-bruno-sportisse-pdg-dinria-donne-quelques-elements-pour-mieux-comprendre-les-enjeux). Thus, it may well be that the technology is used in parts of the world that do not follow strict legal principles, including the declarations of human and citizen rights, laws on privacy, data protection, non-discrimination, etc. These risks are imminent considering that there have just recently been serious impairments concerning the rule-of-law principle even in some EU member states (such as Poland and Hungary).

Notwithstanding the aforesaid, any implementation of the ROBERT protocol under a given jurisdiction, and even the selection of the app supporting device (app, mobile device, wearable, etc.) may entail other legal, cross border, policy, or contractual obligations that have not been subject to this PIA.

PRINCIPLE 2 – ACCOUNTABILITY

In terms of accountability, there may be other risks to consider that come along with third-party dependencies of the applications. These will depend on the security model e.g. of the mobile operating system, which may have access to all data stored in the application provided that such access is allowed by the applicable laws.

Bluetooth is used for contract tracing in ROBERT by using the beacons principle – that is, devices signal each other with short information, without the need to establish a Bluetooth connection between them. Messages are sent to all devices with Bluetooth enabled, there is no ability to send a message to only certain, authorized devices. Thus, it is easy for anyone to listen to everything that happens on the Bluetooth signal. For these reasons, it is possible to spread malicious information. This risk becomes even more crucial considering that the applications

need to be continuously running, with Bluetooth connections activated. Moreover, in order to prevent "one entry" attacks, the server may introduce some randomly selected false positive. In light of the above, accuracy might be at risk and, consequently, it might generate negative consequence where such are not needed (i.e. self-isolation where the contact is not positive). It is noted that several improvements have been made to the ROBERT protocol in an attempt to mitigate or prevent such risks. However, it is impossible to eliminate the risks inherent in using a protocol based on Bluetooth.

PRINCIPLE 3 – TRANSPARENCY AND EXPLAINABILITY

Users have an interest in understanding the risk of intrusive surveillance, long term tracking and the potential for identifying infected individuals, and in the risk scoring algorithm of any particular implementation.

It is possible that the app implementer could also choose to use the algorithm for purposes such as to determine priority of testing or confinement decisions which could have a significant impact on the rights of users.

When a user's positive status is communicated to the central authority it will assign an "at risk" status to the persons who are shown to have come in contact with the positive case. Due to limitations intrinsic to the Bluetooth technology, proximity tracing solutions may lead to false positive and/or negative (see above). The determination of the risk status is therefore subject to the accuracy limitations of Bluetooth technology. In addition to proximity information, risk scores maybe based on other parameters to be decided by the implementor, in collaboration with epidemiologists. The developers of the protocol note that the actual effect of the false positives will depend on the purpose for which the app is being used. They note that a false positive is more problematic if the fact is to notify the user to go into quarantine as opposed to a case where the user is only advised that he or she should get tested.

ROBERT does not require disclosure of adoption rates. It is the idea behind any contact tracing solutions that as many people as possible have respective applications on their mobile devices and keep them activated. Without information available on adoption rates, the efficiency of the Pandemic Tech Solution may be at risk.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

ROBERT is not an application but a communication protocol. One of its design goals is that participants should be able to join or leave the system at any point. The final decision on whether to make the application voluntary or compulsory will be made by the organisations that adopt the protocol. The French Government's present position is that the StopCovid app will be available on a voluntary basis. A final determination is not possible at this stage as the app has not yet been launched.

The requirement of Bluetooth enabled smartphones as the basis of the protocol limits the participation to persons who have access to such devices. In particular, children who do not have their own devices and others such as the elderly and persons with disability who might have trouble engaging with the app could be excluded from the contact tracing mechanism. Accordingly, any conclusions about the aggregate risk profile based on statistics collected from the app may not reflect the cases of persons belonging to these groups.

Depending on the implementation of the ROBERT protocol, false positive results may be of discriminatory effect (see above).

Adherence with the standards and guidelines of the World Wide Web Consortium's Web Accessibility Initiative can help in reducing accessibility barriers in the design and implementation of the solution.

PRINCIPLE 5 – SAFETY AND RELIABILITY

The centralized server structure is the weak point in the ROBERT protocol. Risks of using such centralized system include the following:

Single point of attack: Any breach in a server would endanger the whole federated system and all users of affected applications. Intruding the server could result in the identification of users.

Linkability of users: With a centralized system, the server is able to learn and potentially piece together information about specific users. The server could infer that two infected users were in contact at some point in time based on timestamps, allowing the server to build a partial social graph that reflects these encounters. Furthermore, the server could identify anonymous uploaders with co-locations by performing a frequency analysis on the uploads and cross referencing with who performed the uploads. In addition, the server could identify anonymous uploaders with causality, as causality is preserved in the uploads. Thus, the server can reconstruct a pseudonymous graph using time causality.

Tracing of users: The centralized server creates ephemeral identifiers and can, at any point, link the past and future ephemeral identifiers of any user, infected or not, by decrypting back to their permanent identifier. In combination with other data sets, such as CCTVs, the server can therefore track all individuals, infected or not. Given a target ephemeral ID, such as one collected by law enforcement from a suspect, it is possible to tag and classify individuals that third parties can recognize without access to the centralized server or database. ROBERT's ephemeral IDs are not authenticated, and the server does not provide any proof that they are an encryption of the ID, or that the correct key was used. This capability could allow law enforcement, or other actors, without any access to the backend database, to track the movements of specific users and communities by assigning them distinguishable identifiers and recognizing their tagged Bluetooth emissions. This could enable long-term tracking of individuals or communities (as one could assign specific identifiers to target groups of people) by third parties. Moreover, users could also detect others EBIDs and use them maliciously.

A contact tracing application based on the ROBERT protocol must be widely used and run efficiently to meet the goal of aiding in the containment of the COVID-19 pandemic. However, some characteristics of the present ROBERT protocol give rise to concerns as regards the efficiency of such applications. A technical failure of ROBERT would mean that a user is potentially either not able to share their infected status and thus help notify other users or does not receive notification about having been in proximity to an infected person when queried. In both cases, users may have been exposed, but they will not be notified and thus could be further exposing others by not taking protective measures.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

IP ownership in implementations of the protocol will depend on the choices made by the implementers. Licensing terms of particular implementations (open source or otherwise) will be determined by the implementers.

Under the protocol, data are captured and stored by unique ID/user and EBIDs and by timestamps. The protocol requires sharing of unique IDs/EBIDs in order to map potential infection vectors. The protocol describes NATs (Network Address Translation) as potential mitigation for individual uploads, but notes the limits of NATs both in terms of prevalence and location grouping. The protocol also notes that to ensure network-layer unlinkability, the actual application implementations must be unlinkable using anonymous authentication mechanisms and rate-limiting mechanisms to upload large numbers of observations

PRINCIPLE 7 – PRIVACY

Though many of the above-described risks already could have adverse effects on user's privacy, there are some further privacy concerns that come with the ROBERT protocol.

As outlined before, ROBERT is a protocol, thus a technical basis on which various applications may be deployed. Therefore, any risks would largely be with the implementing apps. However, many of these risks are inherent with a centralized server system. As any application based on the ROBERT protocol would be processing personal data on a very large scale, including sensitive data (namely health data, possibly also data from children or other particularly vulnerable groups), these risks are even more considerable.

Data are stored in the server for three weeks. However, this should be balanced with public health necessities and, in particular, with the pandemic's incubation period. If data retention periods are not minimized, the application based on the ROBERT protocol may infringe the principles of necessity, proportionality and data minimization.

Providing exhaustive and transparent information on the processing of personal data may, under certain jurisdictions or laws (such as the GDPR), be a mandatory legal requirement to observe. However, from the information available on the ROBERT protocol itself, not all mandatory information can be retrieved.

CONCLUSION

The ROBERT protocol with its centralized server structure brings a lot of inherent risks as regards user privacy and data security. Whereas other concerns (such as, for example, regarding non-discrimination, fairness, efficiency) may relatively easy be mitigated by implementing privacy-by-design principles into the applications, the architecture of the protocol itself remains critical. ROBERT may be used for purposes that go way beyond what is necessary in order to mitigate COVID-19, and it may turn out, depending on the organization deploying the application, to become an instrument of mass surveillance.

Although, certainly, also a de-centralized server structure does not come without privacy risks (comp. Serge Vaudenay, Analysis of DP-3T – Between Scylla and Charybdis, Lausanne, 8 April 2020, **https://eprint.iacr.org/2020/399.pdf**), at least the risk of being silently converted into such an instrument of mass surveillance must be considered much lower when using a de-centralized system architecture.

Robert-Koch-Institut (RKI) Corona-Datenspende PostCoviData Impact Assessment ("PIA") Overarching Risk Summary (Key Findings)

May 12, 2020

by Alexander Tribess (Weitnauer Partnerschaft mbB, Germany)

To be read in conjunction with main PIA for Corona Datenspende, dated 11 May 2020.

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

On 7 April 2020, the Robert-Koch-Institut (RKI), the German federal agency for public health, published a corona data donation app for Android and iOS. The RKI app is designed to make users donate to the agency health data from their wearables/fitness bracelets/fitness apps. The RKI aims to derive from such data information on the spread of COVID-19 nationwide and on a regional level.

The goal of the "Corona-Datenspende" (corona data donation) app is to improve prediction possibilities for the nationwide spread of COVID-19 based on unspecific health data (such as pulse rates) and, thereby, to accelerate and focus future containment measures in identified high-risk areas. That being said, the focus of the project is to serve public health as opposed to give the donating user an indication as to whether he or she may be infected.

Considering that testing capacities are limited and, even more importantly, many COVID-19 infections come with only very mild symptoms (so that infected people are unlikely to ever ask for a test themselves, but may, however, spread the virus to others that develop a more severe illness), the RKI aims to better estimate the possible number of undetected COVID-19 infections. The project has been publicly supported by the German Federal Government and, especially, by the Federal Ministry for Health.

Germany can be considered one of the best developed democracies of the world, with a high standard in terms of implementing rule of law. Processing of personal data in Germany (being a member state of the EU) is subject to the GDPR, also for government agencies. In addition, for eGoverment applications, the *Bundesamt für Sicherheit in der Informationstechnologie* (BSI, German federal agency for security in information technology) has published directive BSI TR-03107-1 in 2019, which also apply to the Corona-Datenspende application.

The RKI has been working on this project together with a developing partner from the private sector ; examination of the data derived from the use of the app will be conducted in collaboration with two German universities (Humboldt Universität Berlin, FAU Erlangen-Nürnberg).

The main ethical concerns are that (a) from the data collected through the application, malicious users and/or organizations could get personal health information from a large number of people, (b) malicious users could, by falsifying information uploaded to the RKI, influence and interfere with the containment measures. It is to be noted in this context that the RKI is a direct advisor to the federal government, and its advice is also considered by any other state or private decision-makers ; influencing the data could, thus, have direct effects on public and private pandemic mitigation measures.

Though the individuals directly affected by data processing through the app are limited to users of wearables and other fitness tracking applications (such as iOS Health) voluntarily donating their data to the RKI, the impact of the app on the general public must not be underestimated. The "Corona-Datenspende" app has been developed and published very quickly upon the detection of the first COVID-19 infections in Germany. It has now been available for more than a month and has found a significant number of users (about 500,000).

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

The app being provided by the German federal agency for public health and publicly promoted by the government, its impact on future government measurements to mitigate the COVID-19 pandemic and, thus, its societal and economical effects cannot be underestimated.

Successful attacks on the information security or widespread malicious use of this app have the potential not only to weaken the acceptance of and trust in any app-based measures to contain the pandemic, but they may also cause severe harm to societal and economic welfare in Germany and, considering Germany's importance for the European single market and in international trade, also abroad. Thus, any risks as regards the security of the app create a significant risk to society as a whole, perhaps even on a global level. In addition, any shortcomings in the protection of collected data as well as erroneous forecasts and measures could have a significant impact on the public perception of the RKI itself.

The laws and the legal system in Germany, in general, may be considered sufficient as to mitigate the risks associated to the application. The German federal commissioner for data protection and freedom of information (BfDI) will supervise the deployment and use of this app.

On an individual level, users are free to install and install the app. Depending on the devices they use, they are able to decide which data to share and which to withhold. Users can prevent the app at any time from processing data by switching off or not wearing their wearable. The most important risk for users would be if their share of the data collected by the RKI could be associated with a specific user, i.e. if they were re-identified.

PRINCIPLE 2 – ACCOUNTABILITY

In terms of accountability, it has to be noted that the RKI app is fully dependent on third-party devices or apps. These come with certain risks themselves, the gravity of which will depend on the security model e.g. of the mobile operating system.

The app provider is a software enterprise that has been dealing with eHealth projects in the past. It could have been expected that this provider was capable of implementing mandatory GDPR principles such as, for instance, Privacy be design (Art 25 of the GDPR).

The principles of necessity, proportionality and data minimization allegedly have been observed. However, as it remains unclear which data are being processed exactly and for which particular purposes, it cannot be ascertained whether all data are actually required for these purposes. The lack of explainability certainly constitutes a problem; however, data are said to be transmitted only pseudonymously and anonymized before further processing. It is somewhat typical to scientific processing, that the purposes and the scope of such processing may evolve over time.

Development and deployment are publicly funded. Therefore, if it turned out that mitigating some of the risks identified herein, would come with additional costs, it is very likely that the RKI would decide to spend more rather than accept both avoidable and inacceptable risks.

PRINCIPLE 3 – TRANSPARENCY AND EXPLAINABILITY

As noted above, decisions of the RKI based upon the data derived from the "Corona-Datenspende" may have a huge impact on society. However, the RKI server offers easy ways to create fake pseudonyms with a freely selectable postal code. In addition, knowing the pseudonym of a data donor, third parties can retrieve his authentication token from the RKI server and thus send further data to the RKI under the pseudonym of the data donor, including, for example, the number of steps taken or other activity data. Third parties can also connect their own

fitness tracker and thus their health data with the pseudonym of another user. These risks must not be considered only theoretical because they do not require high-level technical skills. That being said, there is a significant risk (especially in regions with only a small number of users) that data collected through the app may be faulty. This could lead to false predictions in either direction. In terms of transparency, the public most likely cannot and will not be informed about rates of false data input at all.

Though it must never be forgotten that the app is not supposed to serve the individual benefits of its users but the general public, it remains questionable that the RKI provides so little information on the specifics of (algorithmic) data processing operations and the processes of risk analysis. For instance, from the information available so far, users would know that they are to provide their postal code (whereby only the first two digits will be further processed). Furthermore, users know that any analysis from the RKI on the basis of their data will be made on "Landkreis" level. However, this is irritating and requires further explanation as German postal codes are not in any way associated with the "Landkreis" regions (comp. fig. 1 and 2 below, both published in the public domain under CC0 1.0 license). Thus, it remains completely unexplained how the RKI could be able to detect infection risks on a "Landkreis" level on the basis of the first two digits of a postal code. (please note: German postal codes consist of five digits, the first two of which indicate a region of the country that is usually significantly bigger than a "Landkreis", however, big cities are divided into numerous regions, like for instance Hamburg using 20xxx, 21xxx, 22xxx postal codes).

German "Landkreise" (*fig. 1 left*) and German postal code areas (*fig. 2 right*). It can be seen from the maps that sometimes more than one "Landkreis" is covered by a postal code area, whereas in other cases (especially in big cities) one "Landkreis" belongs to numerous postal code areas.
In terms of explainability, it remains entirely unclear how the RKI is supposed to draw conclusions for a "Landkreis" from information based on the first two digits of postal codes.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

The data are collected from an undefined and unrefined group of users. The datasets (especially data on activity levels and data concerning health like pulse rates etc.) cannot be biased themselves. Data are donated by users on a voluntary basis.

Users would never be directly affected by individual decisions of the app or based on the data derived from the app. It would only be possible that, based on information collected through the app, the RKI provides advice to government officials that would then perhaps initiate or lift certain containment measures. Thus, if data input was false or corrupted, individuals, as part of the society, could be treated "unfair".

PRINCIPLE 5 – SAFETY AND RELIABILITY

Technical analysis of the RKI app revealed a variety of major security risks associated with the setup of both the server and the data transfer mechanisms. This revelation is even more concerning as, also considering the communication from the RKI, users are to expect a maximum of data security. As the RKI app processes personal data on a very large scale, including sensitive data (namely health data, possibly also data from children or other particularly vulnerable groups), these risks are even more considerable. The entire model of donating one's personal data for the purposes of serving public health depends on users' trust. Thus, severe shortcomings in data security may endanger the project as a whole.

Any breach in a server would endanger the whole federated system and all users of "Corona-Datenspende". Intruding the server could result in the identification of users. Analysis has revealed obvious shortcomings in server security, though.

The actual data transfer mechanisms for third-party devices and Google Fit are inconsistent with public communications of the RKI. The RKI server gets direct access to and received the data stored on the servers of the fitness tracker provider or data stored at Google Fit. Access data allow access to non-pseudonymized and historical fitness data and, in the case of the providers Fitbit, Garmin, Polar and Google Fit, access to the full names of the data donors, Direct access of the RKI to the fitness data is not even automatically terminated when the smartphone app is uninstalled.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

The app is clearly not designed for data sharing purposes other than with the RKI itself. The data collected through the app will remain with the RKI and its research partners. Data collected through the app are being used for further scientific research on the field of public health.

RKI is mentioned as copyright holder in the iOS app store ; parts of the copyright to the solution, under German copyright law, necessarily remain with the actual developers. That being said, it seems unlikely that the app is going to be distributed to other pubic health agencies in the world.

PRINCIPLE 7 – PRIVACY

Though many of the above-described risks already could have adverse effects on user's privacy, there are some further privacy concerns that come with the "Corona-Datenspende" app.

Consent is implemented by an opt-in procedure (i.e. activating a checkbox underneath the privacy notice). This means that consent shall be declared electronically using non-signature-based processes. However, this is not in line with government agency directives binding on the RKI. Apart from these directives, there have been several Court decisions indicating that consent under the GDPR may solely be valid if the identity of the data subject is undoubtedly clear. Thus, the RKI's approach not to check on user's names in order to keep their identity pseudonymous, may lead to an infringement of data protection principles in itself (Art. 9 para. 2 of the GDPR).

The age limit of the app is set to "4+" at least in the iOS app store, which indicates that the app was designed for use also by small children. During the registration procedure, the user must confirm that he or she was at least 16 years of age. However, this does not constitute an age verification mechanism worth mentioning. Considering that, under Art. 8 of the GDPR, where consent is required in relation to the offer of information society services directly to a

child, the processing of the personal data of a child shall only be lawful where the child is at least 16 years old, this constitutes a crucial weakness.

As the RKI does not actually know its users (see above), there are further shortcomings in terms of mandatory data protection obligations. Any data subject has the right to access information being processed about him or her (Art. 15 of the GDPR) ; data subjects may also request correction or deletion of their data under certain circumstances (Art. 16, 17 of the GDPR). However, any such right may only be granted to a person that can clearly considered to be the actual data subject. Providing access to a data subject's personal data to a person other than the data subject itself would constitute a severe breach of GDPR obligations. Considering that the RKI does not know its users, the only way for the RKI to deal with possible data subjects' requests would be on the basis of the pseudonymous codes being provided to the users during the registration procedures. However, as has been shown, these IDs are neither secret nor protected against unauthorized copying.

The actual data processing operations through the RKI app differ from those stated in the Privacy Policy. Whereas, in the Privacy Policy, the RKI states that (a) data were pseudonymized on the device, (b) no direct identifiers such as names were submitted to the RKI, and (c) data were transferred solely via the user's smartphone, CCC analysis has revealed that quite the opposite is true.

CONCLUSION

The RKI app has the potential of improving the predictability of the spread of COVID-19. However, considering the key role of the RKI within the German response to the pandemic, the data basis for RKI predictions must adhere to the highest standards of reliability. As CCC analysis has revealed, the app itself, its connection to third-party providers, such as health apps and wearables/fitness trackers, and its server infrastructure show some significant shortcomings in terms of data security. At least some of these flaws could have been easily avoided, and it raises some concern that RKI's partners did not implement appropriate safeguards in the first place. Even though some of the deficiencies may have already been cured and others certainly can be rectified, there is a remainder of risks that adversely affect the fundamental human right to privacy as well as the overall reliability and efficiency of the entire app.

In the current state, the "Corona-Datenspende" app must be considered an infringement and the RKI to be in breach of mandatory GDPR obligations, including, without limitation, the principles of data minimization (Art. 5 para. 1 lit. c of the GDPR) as well as integrity and confidentiality (Art. 5 para. 1 lit. f of the GDPR), the accountability obligations of the controller (Art. 5 para. 2 of the GDPR), the lawfulness of processing personal data (Art. 6, 8, 9 of the GDPR), the data subjects' rights (Art. 15 et seq. of the GDPR), the general responsibilities of a data controller (Art. 24 of the GDPR), the core principle of data protection by design (Art. 25 para. 1 of the GDPR), and the obligation to implement adequate technical and organizational measurements to ensure an appropriate level of security (Art. 32 of the GDPR).

Apple/Google Contact Tracing Exposure Notification API Apple/Google API PostCoviData Impact Assessment ("PIA")

June 3, 2020

ItechLaw Evaluation Committee
Charles Morgan, McCarthy Tétrault LLP
Pádraig Walsh, Tanner De Witt Solicitors

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

- "**Apple/Google Contact Tracing API**", in short "**Apple/Google API**", is a comprehensive solution that includes application programming interfaces (APIs) and operating system-level technology to assist in enabling contact tracing.

- Google and Apple announced a two-phase exposure notification solution that uses Bluetooth technology on mobile devices to aid in contact tracing efforts.

- According to the Apple/Google API Exposure Notification FAQ (https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.1.pdf):

  – Both phases of the solution harness the power of Bluetooth technology to aid in exposure notification. Once enabled, users' devices will regularly send out a beacon via Bluetooth that includes a random Bluetooth identifier — basically, a string of random numbers that aren't tied to a user's identity and change every 10-20 minutes for additional protection. Other phones will be listening for these beacons and broadcasting theirs as well. When each phone receives another beacon, it will record and securely store that beacon on the device.

  – At least once per day, the system will download a list of the keys for the beacons that have been verified as belonging to people confirmed as positive for COVID-19. Each device will check the list of beacons it has recorded against the list downloaded from the server. If there is a match between the beacons stored on the device and the positive diagnosis list, the user may be notified and advised on steps to take next.

  – To power this solution in the first phase, both companies will release application programming interfaces (APIs) that allow contact tracing apps from public health authorities to work across Android and iOS devices, while maintaining user privacy. These apps from public health authorities will be available for users to download via their respective app stores. Once the app is launched, the user will then need to consent to the terms and conditions before the program is active. The companies plan to make these APIs available in May.

  – In the second phase, available in the coming months, this capability will be introduced at the operating system level to help ensure broad adoption, which is vital to the success of contact tracing. After the operating system update is installed and the user has opted in, the system will send out and listen for the Bluetooth beacons as in the first phase, but without requiring an app to be installed. If a match is detected the user will be notified, and if the user has not already downloaded an official public health authority app they will be prompted to download an official app and advised on next steps. Only public health authorities will have access to this technology and their apps must meet specific criteria around privacy, security, and data control.

  – If at some point a user is positively diagnosed with COVID-19, he or she can work with the health authority to report that diagnosis within

the app, and with their consent their beacons will then added to the positive diagnosis list. User identity will not be shared with other users, Apple and Google as part of this process.

- According to the Apple/Google API FAQ, if a user decides to participate, exposure notification data will be stored and processed on device. Other than the random Bluetooth identifiers that are broadcast, no data will be shared by the system with public health authority apps unless one of the following two scenarios takes place:
  - If a user chooses to report a positive diagnosis of COVID-19 to their contact tracing app, the user's most recent keys to their Bluetooth beacons will be added to the positive diagnosis list shared by the public health authority so that other users who came in contact with those beacons can be alerted.
  - If a user is notified through their app that they have come into contact with an individual who is positive for COVID-19 then the system will share the day the contact occurred, how long it lasted and the Bluetooth signal strength of that contact. Any other information about the contact will not be shared.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

- Generally, use of the app is intended to help flatten the epidemiological curve of local COVID-19 epidemics and avoid new outbreaks by assisting with contact tracing, while protecting individual privacy.
- Given the emphasis placed on user opt in and voluntary self-notification, and the primacy of human right to health and life, Apple/Google API achieves a balance between rights of the individual and rights of the community.
- In particular, it is designed to be used on a voluntary basis and does not rely on tracing individual movement, but rather on proximity information regarding with respect to other users.
- As we currently understand it, there are no forced auto installs proposed of Apple/Google API, but this will depend on functionality implemented at national levels.
- Subject to national implementations adding functionality, there are currently no automated decision making implications
- The general overarching risk of this app is that (like any other proximity/contact tracing application) it could be used for other purposes post-pandemic.
- We consider that the wider risks of repurposing this app for other state sponsored uses have been adequately mitigated by its distributed architecture. Google and Apple have indicated that they will disable the exposure notification system on a regional basis when it is no longer needed.
- Any other risks (such as for example, the identification and potential singling out of infected individuals and/or those that are required to self-isolate) would be generic to all other contact tracing apps and need to be balanced carefully against the undoubted positive impact to society (and human health) in the use of such technology.

PRINCIPLE 2 – ACCOUNTABILITY

- The API is provided by Apple and Google who will be accountable upon failure. Accountability is also likely to reside with the national health authority adopting Apple/Google API architecture for local/national implementation – ie. ultimately the national government."
- Apple and Google are project sponsors and providers of the API. The front-end apps will be developed by local government or public health agencies
- We have not seen details related to the governance structure for this offering

PRINCIPLE 3 – TRANSPARENCY & EXPLAINABILITY

- As the Apple/Google API system depends on conventional BT LE technology for proximity tracing, the system demonstrates equivalent levels of robustness which would be exhibited by any other distributed network/system.
- The Backend and Authorisation servers should be fully auditable, subject to access being provided by local implementing authorities. We observe that this is not a centralised system – it is highly

distributed. Local data held on smartphones will be outside scope of inspection and audit unless access is granted by (or court orders are sought effecting same).

- Both Google and Apple have published a joint suite of documents aimed at explaining technological features of the API – see apple.com/covid19/contacttracing/ These specifications comprise (i) BT Specification (ii) Cryptography Specification and (iii) Framework API document outlining on a technological basis how they will implement such apps in their OS.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

- The choice to use this technology rests with the user, and he or she can turn it off at any time by uninstalling the contact tracing application or turning off exposure notification in Settings.

- There will be no monetization from this project by Apple or Google.

PRINCIPLE 5 – SAFETY & RELIABILITY

- As the Apple/Google API system depends on conventional Bluetooth Low Energy technology for proximity tracing.

- Bluetooth Low Energy has inherent weaknesses which are capable of exploitation with varying degrees of sophistication, such as noise injection, tracking of users using aspects orthogonal to contact tracing (ie. by logging MAC addresses), wardriving, and theft of mobile phones.

- The system demonstrates equivalent levels of robustness which would be exhibited by any other distributed network/system

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

- The solution has been designed to interoperate internationally.

- Apple/Google have authored an open source reference implementation of an Exposure Notifications server: https://github.com/google/exposure-notifications-server

PRINCIPLE 7 - PRIVACY

- Contractually, Apple/Google API will require to conform to both Apple's App Store standard agreement and Google's Play Store Agreement. Each of these agreements contain separate privacy related terms (Google Play store for example refers to Google's Privacy Policy, see section 9 of that Agreement ; also see section 5.1 Apple's App Store Developer Agreement).

- According to Google and Apple, they have put user privacy at the forefront of this exposure notification technology's design and have established strict guidelines to ensure that privacy is safeguarded:

  – Consistent with well-established privacy principles, both companies are minimizing data used by the system and relying on users' devices to process information.

  – Each user will have to make an explicit choice to turn on the technology. It can also be turned off by the user at any time.

  – This system does not collect location data from your device, and does not share the identities of other users to each other, Google or Apple. The user controls all data they want to share, and the decision to share it.

  – Random Bluetooth identifiers rotate every 10-20 minutes, to help prevent tracking.

  – Exposure notification is only done on device and under the user's control. In addition people who test positive are not identified by the system to other users, or to Apple or Google.

  – The system is only used for contact tracing by public health authorities apps.

  – Google and Apple will disable the exposure notification system on a regional basis when it is no longer needed.

TraceTogether Bluetooth-based contact tracing system PostCoviData Impact Assessment ("PIA") – Key Findings

May 20, 2020

ItechLaw Evaluation Committee
Pádraig Walsh, Tanner de Witt
Philip Catania, Corrs Chambers Westgarth

To be read in conjunction with draft PIA and whitepaper for BlueTrace protocol.

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

- "**TraceTogether**", is a Bluetooth-based application running on the BlueTrace protocol with the aim of assisting and increasing the effectiveness and efficiency of contact tracing. TraceTogether was launched in March 2020 and is downloadable through the Apple AppStore and Google Play.

- TraceTogether will record who a user has been in contact with, but not where. The devices that are running the TraceTogether application will actively communicate with nearby devices and will only record information regarding the proximity of the other device and the duration of the contact.

- Users of TraceTogether are only required to register their phone number with the application. No other personal information is obtained. Upon registration, the user will be issued with a user ID ("**UserID**") for identification purposes.

- A TempID ("**TempID**") is generated by the back-end server to the device on a temporary basis. The TempID is mainly used for communication between devices and only the Ministry of Health of the Republic of Singapore ("**MOH**") has the secret key to decrypt the TempIDs to reveal the underlying UserID, created time and expiry time. The temporary ID is random, anonymized and refreshed at regular intervals.

- Upon a user being diagnosed with COVID-19, the MOH seeks the user's consent to share the stored encounter information to the back-end server (being the TempIDs the user's device has retrieved and stored). The MOH seeks personal confirmation on the physical encounters that the user can remember. The MOH will decrypt the information and analyze the encounters to determine whether they need to be in touch with any other users who have been in close encounter with the COVID-19 contracting user.

- The goal of this project is to assist public health authorities in their efforts to fight the spread of COVID-19 by notifying users of at-risk interactions with patient users allowing potential patients of COVID-19 to be identified in a privacy-preserving manner.

- TraceTogether is designed so that only the MOH will have access to the phone numbers of the users, subject to the user consenting to the sharing of the information. The information collected by the MOH (and on the device) will only be used for COVID-19 contact tracing. It also appears that the MOH is committed to safeguarding the information collected and will not disclose the data to any other users.

- TraceTogether will only collect data on the basis of consent ; the installation of TraceTogether is voluntary.

- The information collected through TraceTogether will not be used to make decisions about the individuals ; rather it will be used (anonymously) to supplement the existing contact tracing practice as adopted by the MOH. It is not intended that TraceTogether will replace the existing manual practice.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

- Generally, use of the app is intended to help control the widespread of COVID-19 and to take patients into treatment at an early stage by assisting with contact tracing, while protecting individual privacy.

- It is designed to be used on a voluntary basis and does not rely on tracing individual movement, but rather on identifying Encounter Information of COVID-19 diagnosed patients to contact other users who may had been in close contact with such diagnosed patient.

- TraceTogether is designed to promote human agency and autonomy

  – Users will have opportunities to provide express consent on downloading the application, allowing the application to send and record Encounter Messages and on sharing such Encounter Messages to MOH.

  – TraceTogether does not process any information collected through the application, it is not designed to operate with AI/ML.

  – TraceTogether does not use any data to diagnose potential patents of COVID-19, instead it merely collects information of whether any other users had been in close contact with the diagnosed patient in order for MOH to contact and invite for diagnosis.

- Strictly speaking, the information to be collected through TraceTogether is limited to non-personally identifying information to reduce the risk of infringing any individual privacy.

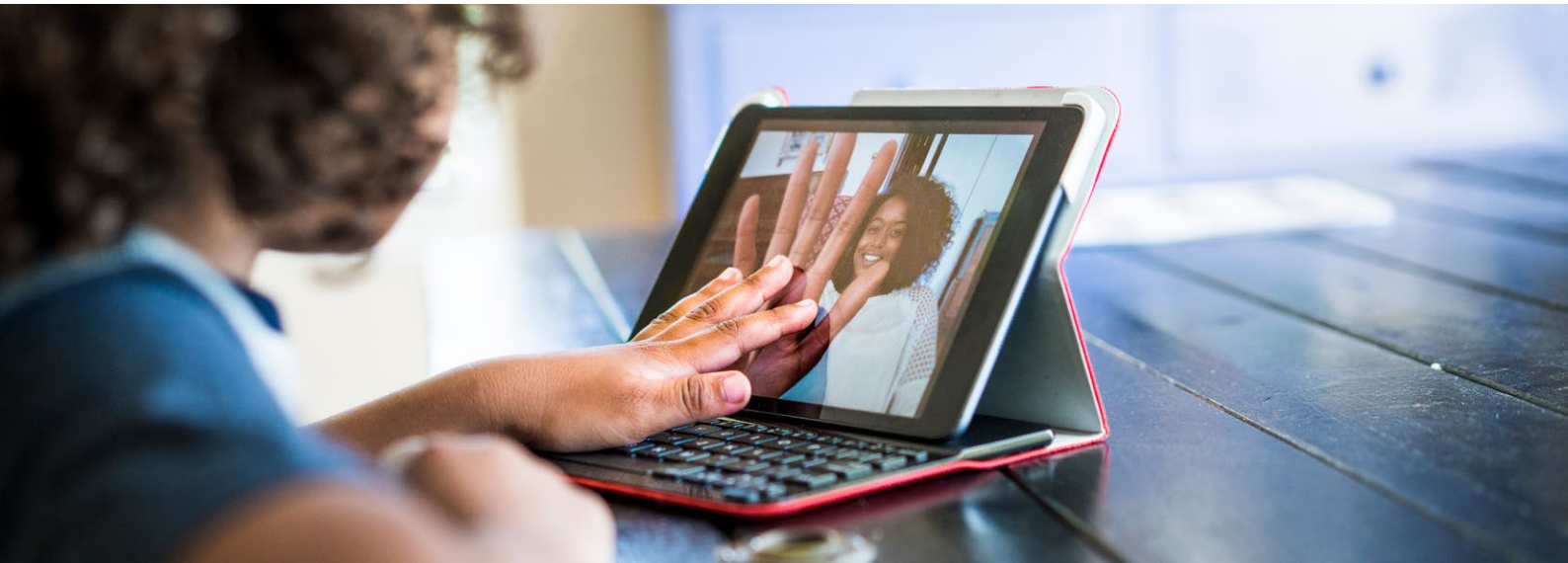
PRINCIPLE 2 – ACCOUNTABILITY

- The government in Singapore is mainly accountable for the operation of TraceTogether.

- Although laudable, this may impact its utility to public health as TraceTogether is deployed internationally. Singapore is a socially cohesive society with a high degree of trust in government. TraceTogether and other applications based on the BlueTrace protocol may struggle for the widespread adoption needed for its success in jurisdictions that do not share these characteristics. Alternatively, other jurisdictions may need to supplement the introduction of TraceTogether with mandatory rules and regulations in order to achieve the intended societal benefit. This, in turn, may create other risks or concerns, especially in relation to accountability.

- For TraceTogether, the White Paper introduces mechanisms to ensure that information would not be intercepted or Encounter Messages would not be intercepted and attacked. Encounter Information stored on individuals' devices are encrypted and TempIDs are generated randomly at intervals. However, the White Paper does not provide any solution or accountability in regards to any flaws in the solution. In particular, Project Owners have received complaints from users who had been contacted by scammers impersonating the MOH.

- Individual phone number and Encounter History, upon consent, are uploaded to the MOH's back-end server where this data is processed manually. Again, the White Paper remained silent on the counter-measures to any security breach in relation to the back-end server. No guidance was given on



how long that information will be retained in the back-end server.

- As mentioned above, one of the key elements to TraceTogether being able to succeed is the high degree of trust the people have in the local government.

- The lack of any specific legislation in Singapore which expressly provides for the protection, restricted use, security and destruction of the personal data will be seen by some as a concern. It may be that from a local perspective, some will not see this as an issue.

PRINCIPLE 3 – TRANSPARENCY & EXPLAINABILITY

- Users will be all members of the general public.

- TraceTogether does not rely on complicated technology. It is built on conventional Bluetooth technology, which has been used by smart phones for years.

- The output of the model can be explained and decisions can be audited.

- No information was disclosed in the White Paper on the provider of the Project Owner's cloud-based backend server. Similar issue was raised for the Australian COVIDSafe app where claims were made that certain US Government agencies are able to access the data covertly and certainly without notice to irrelevant individuals under the US Patriot Act and the US CLOUD Act because the Australian Government contracted with Amazon Web Services for the provision of back end server.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

- There is no concern in relation to fairness & non-discrimination of TraceTogether. It is solely up to the MOH to decide how to process the information released by the consenting users. This is a matter of government policy in dealing with the pandemic instead of an issue of the Pandemic Tech Solution.

- TraceTogether will collect all Encounter Messages in the device's proximity, as long as TraceTogether is being installed.

- Concerns have been expressed that people who do not have mobile devices or mobile devises capable of downloading and operating the TraceTogether App are at a clear disadvantage. Notwithstanding the high level of mobile device proliferation in Singapore, there are some people (particularly certain senior citizens who of course are in the significant vulnerability group) who are unable to utilise the App

PRINCIPLE 5 – SAFETY & RELIABILITY

- The success of TraceTogether is significantly dependent on users providing a valid phone number upon registration and having the device with TraceTogether installed with the user at all time in order to produce reliable results. This is further restricted for users with a device that operates the iOS operating system (i.e. Apple) as BlueTooth technology does not operate in the background on iOS. This is an issue for which the Project Owner is still seeking a solution.

- The privacy safeguards will also have direct impact on the reliability of the Pandemic Tech Solution as many steps in between require manual input by users and the MOH, for example what happens if the user does not pick up the phone when being contacted by the MOH ?

- The White Paper is also silent on the effectiveness of the Pandemic Tech Solution, especially in a crowded area where BlueTooth technology may not operate as efficiently.

- The device must also be connected to the internet for at least once per day in order for the back-end server to generate sufficient numbers of TempID to be used by TraceTogether. Expert opinion suggests that, to further minimize any risk of attacks, TempID should be generated locally on individual's device.

- Data collection process is designed to render replay/ relay attack difficult, but this does not seem to be a watertight solution.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

- The solution has been designed to interoperate internationally. There are mechanisms built to allow exchange of information between different

public authorities from different jurisdictions but it is unclear how this will function at the moment.

- Presently, it is not intended for the Project Owner to launch the solution in jurisdiction other than Singapore. Users from the United States and United Kingdom would be able to install and run the application provided they have a Singaporean phone number.

- The BlueTrace protocol is open sourced and the Project Owner has indicated that any other jurisdictions are free to implement locally as they deemed appropriate. This includes the COVIDSafe application launched by the Department of Health of the Australian Government.

PRINCIPLE 7 - PRIVACY

- Although this may impact the effectiveness of the Pandemic Tech Solution, the solution is designed to protect privacy data.

- Pseudonymized data (i.e. phone number) is required for the operation of TraceTogether. The Project Owner will have no other information (include the name of the owner of the phone number) even when given consent to access the data collected through TraceTogether.

- There are measurements in place to ensure that even the pseudonymized data would be difficult to be intercepted or have any value to attackers. However, it is our view that there are still areas of concerns in relation to a leakage of personal data, especially for attackers with malicious intention. Re-identification may still be possible (i.e. if the attackers managed to decrypt the TempID to retrieve the phone number of the devices and hacked the database of telecommunication companies to re-identify the user).

- Whilst the information collected does not reveal GPS or geological location, it may give rise to other valuable information such as the identity of other users that one user meets on a regular and frequent basis.

- Nevertheless, the solution is intended to fully comply with the existing privacy law. Users are able to revoke their consent at any time, and all information collected would be deleted automatically thereafter. Moreover, information will only be stored on an individual device for not more than 21 days, after which it would be automatically deleted immediately. But the White Paper is silent on the availability to users on accessing, reviewing and correcting the information stored in the device and stored with the back-end server after initial consent was given.

- Singapore has not introduced any amendments to its privacy legislation in relation to data generated by the contact tracing App. It appears that there are no plans at all for amendments to the Singapore Privacy Act. Rather, the Singapore Health Ministry's contact tracing activities and the use of collected data are already subject to sectoral rules in place under the Singaporean Infectious Diseases Act. It would also appear that collected data would be protected from misuse under the Singapore Official Secrets Act but, as mentioned, these are not specific privacy related pieces of legislation

- In contrast, privacy of data generated by the Contact Tracing App has generated significant political and social commentary in Australia. There has been a number of very prominent privacy academics and professionals who have publically stated their concerns with the privacy statements made by the Government and the privacy regulations that are being promulgated. This will have actively discouraged a number of people from downloading the App (although at the time of this key finding, there are over 5 million downloads of the App in Australia). Nonetheless, a number of high profile politicians and other people have stated that they won't be downloading the App because of privacy concerns. In response to this, the Federal Government of Australia issued a Determination (which has the effect of legislation) introducing certain privacy protections in relation to data generated by the App – including, for example, the fact that the data must be encrypted, it can only be accessed by certain personnel, it must be destroyed within a certain amount of time and so on. In addition, the Federal Government late last week issued an exposure draft of amendments to Australia's Privacy Act to give further effect to the Determination and to extend privacy protection. In other words, Australia is treating privacy protection in relation to data generated by the contact tracing App as something within the purview of Australia's privacy laws.

Nodle Coalition PostCoviData Impact Assessment ("PIA")

June 1, 2020

ItechLaw Evaluation Committee
Belén Arribas
Massimo Donna

To be read in conjunction with Privacy Impact Assessment and whitepaper for COALITION App ("**COALITION App**").

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

- COALITION App ("**COALITION App**") is designed to allow contact tracing in the general populace and proposes an architecture which is capable of international deployment.
- Coalition was conceived with an international audience in mind, therefore its creators are keen to deploy it internationally. As such the countries which take it up may have differing legal contexts and backgrounds, including in relation to general rules of law. In light of the above considerations, since Coalition may be deployed in non-democratic or quasi-democratic countries, potential deployment risk is high.
- Since Coalition may be deployed in non-democratic or quasi-democratic countries, potential deployment risk is high.
- Market/industry/sector – General use application. The app is intended to be used across all aspects of society and industry by all citizens that possess a smartphone.
- Main regulatory requirements – Data Protection (GDPR and associated legislation such as ePrivacy directive); laws applicable to the use of telecommunications networks; laws applicable to privacy, individual and mass surveillance.
- Main ethical concerns: Privacy, Right not to be discriminated against, government surveillance.
- Auditability is yet to be confirmed, but **the source code will be made open source** and publicly available for scrutiny.
- The impact of **Coalition App data processing activity is significant** – it will enable citizens who have sufficiently uptodate smartphones to understand the risk of whether they have been in contact with other infected (or potentially infected) individuals and remove them from the chain of infection by means of **notifying them to self isolate and recommending actions to mitigate against risk, including self-isolation**.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

- Coalition aims to provide an effective solution to fight the COVID-19 crisis, while protecting individual privacy.
- In particular, Coalition is designed to be used on a voluntary basis and does not rely on tracing individual movement, but rather on proximity information with respect to other users.
- Although the system relies on the collection of information that cannot be linked to individuals (non-personal data), such information

may relate to the health of the Users, if they decide to upload their data further to testing positive.

- The Coalition App will only be downloaded and installed by Users on a voluntary basis.

- All processed data will be anonymised and Users will only notify the back-end server of their having tested positive for COVID-19 on a voluntary basis.

- These factors significantly reduce the risk of citizens' right to data protection being breached or that citizens may be discriminated against. Generally, use of the app is intended to help flatten the epidemiological curve of local COVID-19 epidemics and avoid new outbreaks by assisting with contact tracing, while protecting individual privacy.

- The solution generally complies with the ethical purposes of beneficence and non-maleficence. However, the general overarching risk of this app is that (like any other proximity/contact tracing application) it could be used for other purposes post-pandemic (i.e. for state surveillance purposes).

PRINCIPLE 2 – ACCOUNTABILITY

- The role of Nodle, from a legal standpoint, has not been clarified, hence accountability criteria are not clear.

- Major third party dependencies include:

- OS providers – Apple and Google

- BT LE System infrastructure and specification

- OS provider and BT LE infrastructure risks have already been previously identified.

- There are no third party data sources as SKs and TIDs identifiers are generated by user handsets.

- In the White Paper it states that User can, at any time, request access to the personal data that relates to User. It states further that such data are, e.g. phone number and associated random IDs. It is unclear whether a method for correcting personal data is provided

PRINCIPLE 3 – TRANSPARENCY & EXPLAINABILITY

- Users will be all members of the general public without any heightened technical sophistication.

- Data are not proprietary – they are ephemeral identifiers: ie pseudo randomised BT LE (Bluetooth Low Energy) data packets.

- The Backend and Authorisation servers should be fully auditable.

- However note that this is not a centralised system – it is highly distributed. Local data held on smartphones will be outside scope of inspection unless access is granted by (or court orders are sought effecting same).

- As the Coalition system depends on conventional BT LE technology for proximity tracing and TIDs are auto generated by phone handsets, the system should demonstrate equivalent levels of robustness which would be exhibited by any other distributed network/system.

- Coalition is susceptible to BT hacking and other cyber-risks.

- These risks are not unique to Coalition but are generic to distributed solutions of this nature.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

- Although certain current aspects of the Coalition solution do not seem to be consistent with its stated characteristic of only processing anonymized personal data (i.e. during the installation process and when user self-declares positive, the app requires user's mobile phone number), the general understanding is that when deployed in a "production" environment, no personal data as defined under the GDPR will be processed. Thus, no automated individual decision making or processing as per article 22 of the GDPR will be involved in connection with the Coalition app deployment and no AI-induced discrimination appears likely.

- However, a more basic form of de facto discrimination may arise as certain segments of

the population either by reason of age, census or disability are not in a position as to own or appropriately handle smartphones or other digital devices upon which the app must be installed.

PRINCIPLE 5 – SAFETY & RELIABILITY

- Coalition, as an anonymous solution is theoretically subject to coordinated collective hacking conduct, where, for example, a number of individuals self-declare infected even if not tested positive for coronavirus with a view to sabotaging the solution. Although the likelihood of such a coordinated scheme is unlikely, should it be implemented it may cause widespread distress to people who are notified of having been close to infected individuals, even if this is not the case.

- Certain security risks have been anticipated in connection with the cryptographic technology used by the app developers, however such risks require a "tech savvy" and malicious bad actor.

- Conversely, major risks may be associated to the general population potentially attributing to the app reliability and robustness which may prove ephemeral, since they are dependent on a number of factors, including the app installation and adoption by a significant share of the populace.

- Our recommendation is that a programme of public awareness and education should be implemented in a manner befitting of the wide spectrum of public consumption.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

- The solution has been designed to operate internationally.

- The solution will be made available subject to an open source license.

PRINCIPLE 7 - PRIVACY

- Whereas it might be opined that users' data are not truly anonymized, but only subjected to hard pseudonymization, it appears that only extremely tech-savvy bad actors may succeed to re-identify users' personal data.

- Therefore, it might be argued that anonymized data fall outside the field of application of the GDPR and of other data-protection legislations in the West.

Arogya Setu App ("Pandemic Tech Solution") PostCoviData Impact Assessment (“PIA”) Overarching Risk Summary (Key Findings)

May 12, 2020

by Nikhil Narendran (Trilegal, India)
Smriti Parsheera
Swati Muthukumar (Trilegal, India),
Aparajita Lath (Trilegal, India)

To be read in conjunction with main PIA for Arogya Setu App.

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

The Pandemic Tech Solution (or **Solution**) is a mobile application developed by the Government of India with private partnership. The app developers describe it as a solution to connect essential health services with the people of India to fight against COVID-19. The Pandemic Tech Solution’s terms note that it is “*aimed at augmenting the initiatives of the Government of India, particularly the Department of Health, in proactively reaching out to and informing the users of the app regarding risks, best practices and relevant advisories pertaining to the containment of COVID-19*”. Further, the App's terms of use also state that the App will serve as a digital representation of an e-pass where available. The App will also provide links to convenience services offered by various service providers.The key features of the Pandemic Tech Solution include contact tracing, self-assessment by users and integration of e-pass for movement during the lockdown. The Pandemic Tech Solution uses the user's Bluetooth and GPS location data to carry out contact tracing and the underlying structure of the Pandemic Tech Solution is largely centralised. The data collected by the Solution is highly sensitive as it contains personal information including health status, location etc. albeit in a de-identified format.

The Solution may have a significant impact on the user's right to privacy, which constitutes a fundamental right. The Pandemic Tech Solution is citizen-facing. By way of notifications issued under the Disaster Management Act, 2005 (**DMA**), the Government of India has directed employers to ensure that the Solution is installed by employees on a best effort basis and empowered district authorities to advice individuals to install the Solution. While the DMA contains broad powers on measures that may be taken in response to a disaster situation, there is no specific enabling provision under the DMA which expressly permits any curtailment of the right to privacy. There are also questions as to the legal oversight of the Solution, particularly in light of the fact that India has no overarching data protection law. As per the Data Access and Knowledge Sharing Protocol, 2020 (Protocol) released by the government, the Pandemic Tech Solution may be used to make decisions in relation to sharing of a user's data for (i) directly formulating or implementing an appropriate health response, (ii) to assist in the formulation or implementation of a critical health response, or (iii) for research purposes. The Protocol also lays down other principles for the collection and processing of the data. However, the Protocol itself does not have any specific legislative basis and can be modified at any point by the Empowered Group that notified it.

Stakeholders impacted by the Solution are citizens (end users), employers, universities/research institutions or entities, government and healthcare personnel.

The Government of India along with its private partners is responsible for the Pandemic Tech Solution and departments or officers may be held responsible for certain non-compliances under the DMA. The terms of use state that the Government will make best efforts to ensure that the Solution performs as described. However, the Government will not be liable for (a) the failure of the Solution to

accurately identify persons who have tested positive to COVID-19 ; (b) the accuracy of the information provided by the Solution as to whether the persons who users have come in contact with have in fact been infected by COVID-19. This impacts the extent of responsibility and control which may be expected from the Government.

The Pandemic Tech Solution reportedly has 114 million downloads and likely a similar number of users. The data is collected constantly and it has the potential of becoming a tool of mass surveillance. The impact of processing the data is significant, as it will enable the government to understand whether Solution users have been in contact with other infected individuals and potentially remove them from the chain of infection by quarantine or isolation. It may further allow persons carrying out medical and administrative interventions necessary in relation to COVID-19 the information they might need about the user in order to be able to do their job.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

The Solution has been provided by the Government of India to aid the response efforts to the COVID-19 crisis in India. Though employers and district authorities are required to ensure that the Solution is installed on a best effort basis. This could lead to a situation where employees / individuals are left with no option but to install the Solution. This may negatively impact human agency and autonomy and may have implications on a user's right to privacy and may result in loss of livelihood should they choose not to use the Solution, including by way of criminal prosecution under the DMA.

The absence of an overarching data protection law and a legislative backing to the Solution raise concerns on the legal implications and risks of harm to users. In addition to this, there is the general overarching risk of surveillance related use, false negatives, unauthorised access to data (including health data) and triangulation of user location. However, there are efforts being made to limit the period of data retention by the Solution and the manner in which data sharing can take place, which will reduce these effects to an extent.

PRINCIPLE 2 – ACCOUNTABILITY

The Solution, as initially released on 2 April 2020, was not open source and reverse engineering was also prohibited. However, the reverse engineering restriction has been removed and the Solution has been made open source at the source code level (for Android only) on 26 May 2020 i.e. nearly two months after its release. The terms of service permit users to report defects or bugs in the Solution to the Government. Given that the Solution was made open source, at the source code level, only after 26 May 2020, the App's code has not yet been audited by independent third parties. The Government has announced a bug bounty program (open till 26 June 2020) and anyone who reports vulnerabilities with the Solution will be awarded up to INR 400,000. Further, in order to ensure accountability, the Solution must also share information on the server-side code/centralization processes.

It is therefore difficult to comment on the accountability of the Solution As the Solution strives to achieve multiple purposes such as aiding both users and government authorities in responding to the COVID-19 threat, it is also difficult to determine whether the data collected is necessary and limited to such purpose.

The Solution also does not extensively apply the Privacy by Design model. This is evidenced by the fact that some users are forced to create an account and provide their data to the Solution, there is an absence of a mechanism to delete their account and the Solution collects data and stores it along with the user's personal data. While the period for retention of an individual's data by the Solution is limited and specified in its terms and the Protocol, the Solution itself does not have a defined retention term.

PRINCIPLE 3 – TRANSPARENCY AND EXPLAINABILITY

There is a lack of transparency about the process of development of the Solution, including details of the private individuals and organisations that assisted the government in this initiative and the alternatives that were considered. There is also very little transparency on the Solution's use of information, accuracy of outcomes, etc. as the Solution's code (for Android

only) has only recently been made available for audit and the Government of India has not provided updates on the system architecture, data sets, processes or results. However, the Government has identified the manner in which the data collected from the Solution shall be used and the time period for which it may be retained. It is essential that the Government provides similar transparency on the Solution itself, and provides information such as the audits undergone by the Solution, the manner in which it makes decisions, etc.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

The Solution does not meet accessibility standards. It is not possible to determine the quality of decisions made by the Solution at this stage due to insufficient availability of public information.

PRINCIPLE 5 – SAFETY AND RELIABILITY

The Pandemic Tech Solution has recently been made open source at the App source code level (for Android)and is largely centralised. The Solution, as initially released on 2 April 2020, was not open source and reverse engineering was also prohibited. However, the reverse engineering restriction has been removed and the Solution has been made open source at the source code level on 26 May 2020 i.e. nearly two months after its release. The terms of service permit users to report defects or bugs in the Solution to the Government. The Government has announced a bug bounty program (open till 26 June 2020) and anyone who reports vulnerabilities with the Solution will be awarded INR 400,000. Given that the Solution was made open source at the source code level only after 26 May 2020, the App's code has not yet been audited by independent third parties. Further, open sourcing has been selective and the server side source code is still not open source. There is not yet enough data on whether the Solution is functioning in the exact manner that has been specified by the government. There are news reports of ethical hackers pointing out security issues in the Solution. While these claims have been disputed by the Solution's developers, it is difficult to comment on the veracity of the claims of either side without the Solution's code being audited by multiple independent researchers.

With respect to information security certifications, the Protocol requires entities handling the Response Data to implement the ISO/IEC 27001 standard. Further, data is encrypted in transit as well as at rest. However, insufficient information is available relating to secure software development and details of implementation of encryption measures.

The privacy policy of the Solution specifies certain use restrictions. Data will be used only by the Government of India in anonymised, aggregated datasets for the purpose of generating reports, heat maps and other statistical visualisations for the purpose of the management of COVID-19 in the country or to provide users general notifications pertaining to COVID-19 as may be required. There exists a possibility of subversion of intended use and extended state surveillance. The Government of India requires employers to ensure that employees install the Solution on a best effort basis and district authorities are also empowered to advise individuals to install the Solution. Consent will be invalid if used as part of mandatory enforcement. There is not enough data to comment on whether the Solution can be used for dual purposes.

As the Pandemic Tech Solution processes personal data on a very large scale, including sensitive data (namely health data, possibly also data from children or other particularly vulnerable groups), any breach in security measures could violate user privacy as well as endanger the whole centralised system.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

Information on the scope of interoperability with tech solutions offered by other providers is insufficient. As per the privacy policy and Protocol for the Solution, data will be used only by the Government of India, public health institutions, Indian universities / research institution and onward transfer to third parties is restricted. Further, reuse of data for other public interest projects is also restricted as per the Protocol. Information on ownership or intellectual property rights attaching to the Pandemic Tech Solution is insufficient. At this point there isn't enough information to assess whether the Solution or data gathered by it could be distributed to other public health agencies in the world.

PRINCIPLE 7 – PRIVACY

Many of the above-described risks have adverse effects on user's privacy. The Government of India requires employers to ensure that employees install the Solution on a best effort basis and district authorities are also empowered to advise individuals to install the Solution. Consent will be invalid if used as part of mandatory enforcement. Further, children and vulnerable groups are included and there are no security safeguards for processing of the information of such groups.

While the privacy policy and the Protocol specify a data retention / deletion procedure, currently, there is no option to de-register or logout from the Solution. Since the personal data will be retained as long as the "account remains in existence", there is currently no way of ensuring that the personal data is deleted from the Solution.

There is insufficient data with respect to assessing whether beyond the data subject, the privacy of an identified group be at risk. The Solution is not very clear on what the consequences of a "yellow" or "orange" report are with respect to the self-assessment test to be undertaken on the Solution. As per the privacy policy, every time the user completes a self-assessment test, the Solution will collect their location data and upload it along with the DiD to the server. While the stated purpose is that this information will be used by the government to evaluate whether a disease cluster is developing at any geographic location, due to the lack of clarity around yellow/orange reports, it is unclear if this will be used to identify the probability of a user having COVID-19 or for any other testing-related purpose or may also expose identified group to be at risk.

There is insufficient data to show whether individuals are aware of observation at some point in time and whether and how new data is created.

CONCLUSION

The Solution has the potential of improving the predictability of the spread of COVID-19. However, since the Solution has been made open source (for Android only) at the source code level recently, there is insufficient data, as yet, on whether the Solution adheres to the highest standards of safety and reliability. However, initiative like the bug bounty program are steps in the right direction to encourage investigation of the Solution and to report vulnerabilities. Reports have highlighted significant shortcomings in terms of data security but these claims have been rebutted by the Government. Even though some of the deficiencies may have already been cured and others certainly can be rectified, there is a remainder of risks that adversely affect the fundamental human right to privacy as well as the overall reliability and efficiency of the entire Solution.

Further, as employers / district authorities may make it mandatory of individuals to install the App, the consent framework for collection of personal and sensitive personal data remains questionable. The Pandemic Tech Solution is not geared for use by people who are differently abled. Given that the Solution may be made mandatory for its use for various activities such as for right to access work place or travel, the solution is in-accessible to a large number of people. The Solution is not transparent or explainable and a person impacted with a false positive has no institutional process to challenge it. In terms of legal protections and remedies, there is no specific legal framework in place for holding the government accountable for privacy breaches except general constitutional remedies that flow from the recognition of privacy as a fundamental right.

Estimote, Inc. Workplace Safety Wearable Overarching Risk Summary (Key Findings)

May 12, 2020

by Jenna F. Karadbil (Law Office of Jenna F. Karadbil, P.C., New York, NY, United States) with contributions by Doron Goldstein (Katten Muchin Rosenman LLP, New York, NY, United States) and Dean W. Harvey (Perkins Coie LLP, Dallas, TX, United States)

To be read in conjunction with the PIA for Estimote's Workplace Safety Wearable, dated May 15, 2020. There is very little public information available on the Estimote wearable solution, so this review has been based on the available documentation, the CEO's interview and third party documentation, both cited in the PIA.

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

In early April 2020, Estimote, Inc. launched its workplace safety wearable device solution to assist companies with contact tracing and identification of infected or exposed employees. Estimote is a for-profit company based in Krakow, Poland that was formed in or around 2012. The solution aims to help companies save money by maintaining a safe workplace and quickly identifying and resolving risks. The solution is a modification of an existing "panic button" wearable, which, when deployed with other Estimote beacon technology, is used by employees to alert management to an event, with the Estimote beacons identifying where in the company building the employee is experiencing such event. The new workplace safety wearable is virtually the same hardware, with new code snippets created to add in the contact tracing and health identification services.

The goal of the Estimote solution is to identify infected or symptomatic employees (by virtue of their pressing a button on the wearable) and accelerate and focus containment measures by the company both for exposed employees and in the identified areas of the company. The solution is fully dependent on the infected or symptomatic employee reporting their positive COVID-19 diagnosis or experiencing of symptoms. The backend of the solution cannot serve its actual function without obtaining such information from the infected employee's wearable device. The solution is not currently customer or publicly focus, and is instead intended to be used solely within a company's physical locations.

The Estimote solution stores information, presumably employee names, locations, durations in locations, contacts with other employees, and healthy status. No specifics of the solution have been released ; thus it is unknown what information is stored on the wearable, transmitted from the wearable via cellular network to the backend, and is maintained on the backend. There is no information as to how long all of this sensitive information is stored, how it is stored, where it is stored, who has access to it, whether it can be exported or shared, and whether Estimote will have access to or host any of the implementing companies' data or systems.

Because the Estimote solution is meant to be used by companies world-wide, it is possible that several countries' laws and regulations would apply both to Estimote and the implementing companies. As such, there is an inherent risk for employees where the solution is deployed in countries that do not have strong (or any) data protection laws and regulations, workplace monitoring and safety laws and regulations, laws against discrimination, telecommunications regulations, collective bargaining agreements, regulations for wearable devices, regulations for medical devices, and protections from mass surveillance.

The main ethical concerns are that (a) mandatory usage and sharing of employee health data, (b) employee privacy, (c) transparency about who can see and use the data, (d) security of the data, and (e) what else it might or could be used for outside of the intended purposes. These concerns are further compounded by the fact that each company

that implements the solution is responsible for its own implementation, unless Estimote assists in operating it or providing its hosted cloud services for the backend of the solution.

Though the individuals directly affected by data processing are limited to users of the wearable device, voluntarily providing their data to their company, the solution could have an impact on the general public by helping implementing companies quickly identify and contain possible outbreaks. The Estimote solution was developed and deployed very quickly upon the COVID-19 crisis becoming a worldwide pandemic. It has been deployed in several companies, though no usage or deployment data has been released by either Estimote or any of the implementing companies.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

The Estimote solution is being deployed to protect employees from other employees by enforcing social distancing guidelines, alerting companies to employees that fail to comply with social distancing guidelines, and to help quickly identify potential exposures and attempt to contain further exposures in the workplace. The Estimote solution aims to assist companies, not the general public, though, as noted above, the implementation of the solution by companies could have a positive impact on the general public by helping to identify and contain possible outbreaks. Further societal benefits could include helping employees come back to the workplace from being furloughed or in an unpaid status, help employees and their family members feel safe both in their workplace and at home knowing they have not been exposed at work, helping companies maintain clean workplaces and products both for employees and customers, and if tests are limited, help identify those employees that should be tested based on their exposure(s).

There is minimal autonomy provided to the employee in that they have the option to not wear the device, to turn it off or to let it die and not replenish the charge. In practice, however, there may not be any actual autonomy, as employee's work or job retention may be based on mandatory usage. Importantly, the entire solution may not work effectively if employees choose to opt-out of wearing the device, as it would not be able to effectively contact trace potentially exposed employees or locations. While employee data is said to be anonymized either on the device or in the transmission from the device to the backend, the Estimote dashboard makes de-anonymization appear very easy. Employees also would appear not to have any control (or potentially even knowledge) of how, where, when, and by whom, their personal data is de-anonymized and shared.

Although Estimote intends for the wearing of the device to be voluntary, doing so may adversely affect the solution's efficacy. Thus, there is a conflict betweeen employee autonomy and effectiveness of the solution.

Successful attacks on the information security or widespread malicious use of the device and its data have the potential to weaken the acceptance of and trust in the solution to contain the pandemic at the workplace. If the solution is easily hackable or manipulated, does not work as intended, or is used for uses not consented to, then it could affect both Estimote's and the implementing companies' reputation and business.

The use of a centralized system increases the risks of attacks and that data collected through the device and on the backend could be used for unintended purposes, including nefarious purposes, such as surveillance and location tracking outside the workplace.

Because each company will have its own implementation of the Estimote solution, it is possible that other legal, cross border, policy, or contractual obligations could apply that have not been mentioned or reviewed in this PIA.

PRINCIPLE 2 – ACCOUNTABILITY

In terms of accountability, the Estimote solution is largely dependent on third-party company implementations since the solution is fully programmable by the implementing companies. Estimote has not disclosed what portions are not customizable. These risks are unknown, as company implementations appear to be private, and should arguably at least stay somewhat private, to help protect their employees' sensitive information.

This appears to be Estimote's first foray into a device aimed specifically at a health crisis, though the originating panic button device could be used to notify of a health-related event or emergency. It is unknown how or whether there will be any support provided for the solution, including if employees have issues with the devices or companies have issues with the backend or customization.

Importantly, Estimote has not updated its Privacy Policy since 2015, including not making any adjustments after the enactment of GDPR, including in its home country, Poland. The Privacy Policy does not mention or appear to apply to the wearable solution.

The principles of necessity, proportionality and data minimization have not been disclosed. No privacy measures have been disclosed, other than the fact that data will be transmitted in anonymized form to the backend, and viewable in the backend in anonymized form until the company wishes to de-anonymize it. The company could potentially use and share the de-anonymized data for both intended and unintended purposes.

Development and deployment are funded by Estimote, a private company. Therefore, if it turned out that mitigating some of the risks identified in this PIA would come with additional costs, it unknown whether Estimote would decide to spend more rather than accept both avoidable and unacceptable risks. Though, not doing so could have an impact on its reputation and business.

PRINCIPLE 3 – TRANSPARENCY AND EXPLAINABILITY

While there is transparency in use of the device, as an employee can clearly see who is wearing one, there is very little transparency with respect to everything else about the solution. Further, an employee should assume that at least some of his or her personally identifying information is stored and processed by the back end, as that would be inherent in any properly working contact tracing solution.

It is unknown how or what personally identifying information of the employees is contained in the solution, and employees appear to generally not have access to any of their data stored or used by the solution. However, each implementation will be based on the specific implementing company's existing data and requirements.

There are no specific Terms of Service for the Estimote solution. Estimote's existing Terms of Service are from 2015 and do not mention or appear to cover wearables. While Estimote's undated Terms of Sale appear to apply to other Estimote goods, they do not specifically mention the wearable solution, nor do they mention the predecessor it was based on – the panic button solution.

It is unknown what terms will apply for employees that use the device, as the company that implements the wearable will likely be entering into the agreement with Estimote, not any individual employees. Thus, employees could then be subject potentially to Estimote's terms, but also any terms and/or policies of their employer.

While the general solution is fairly explainable, it does not include specifics as to the wearable or backend, or to any company's implementation.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

In terms of accessibility, the device should be able to be used by any and all persons, as it is wearable either on a neck lanyard, wrist device, or as an access card. Since the wearer does nothing but turn it on, it should be usable by anyone, including those with limited capacity or ability.

The quality of the data is subject to the veracity of the employees using it as well as the potential accuracy limitations of Bluetooth and LTE technology. Thus, there could be reporting of false positives and corrective action taken, when, in fact, it was not actually necessary. Or, failures to report in order to maintain one's job or paycheck, which could expose other employees and sites within the company. So, there is a risk that employees will purposely not report, though less of a risk that employees will falsely report, their infected statuses.

The quality of the data is also subject to proper functioning of the wearable, transmission means and the backend. If the device malfunctions and a report is not registered or transmitted to the backend, then employees would be left open to potential exposure and great health risk.

Because companies can collect location data, not just for purposes of contact tracing, its usage could be unfair and/or used in a discriminatory manner.

PRINCIPLE 5 – SAFETY AND RELIABILITY

Very little technical data has been released, so no technical analysis of the Estimote solution has been performed, including assessing the security and reliability of the solution. This is very concerning, as employees are likely to expect their person and sensitive data to be both secure and accurate. The wearable is relatively new, with the prior device having been released just a few years ago. No reliability or security data has been released on the original device, or this new workplace safety version.

Employees are at risk of their data being disclosed and potentially used for unintended purposes. An employee's infected status could be made public without their authorization. Or, an employee could be tracked outside of the company or during non-working hours to create a full picture of each of the employee's movements.

The backend contains all of the data from the wearables, plus additional identifying data about the employees. A breach of the centralized server could lead to revealing all of the data and personal information contained in the solution. Each implementing company will be responsible for securing their own environment, unless they utilize Estimote's cloud hosted environment, in which case Estimote should have primary responsibility. It is unclear whether Estimote will have access to a company's data, in addition to the implementing companies. It is also unclear whether the data will be shared with any third parties, as the Privacy Policy is so old that it does not cover this wearable solution. It is possible that the device could also transmit data back to Estimote, or elsewhere, not just to the company that has implemented the solution.

Although unlikely, the device could be considered a medical device and then would be subject to medical device regulations. Particularly, if the company customizes the implementation to be assisted in its function by pharmacological, immunological or metabolic means. However, the EU has extended the time period for compliance with its medical device regulations until next May.

Although Estimote has noted that the data is securely transmitted from the device to the backend, no information as to how this is accomplished has been disclosed.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

The Estimote solution is proprietary and owned by Estimote, including all intellectual property, as no parts of it appear to be open sourced. Currently the solution will be used solely by Estimote's company customers, though public health uses are being explored. Companies will likely enter into some form of a license agreement with Estimote for the use of the wearable and the backend. Users may then be subject to their employer's policies or agreement with respect to their use of the wearable.

As noted above, it is unknown whether Estimote will have access to the data collected by the device

or processed on the backend, in addition to the implementing company. The device is not meant to do anything other than its intended purpose, however, it is fully programmable and thus can be altered to serve other purposes.

PRINCIPLE 7 – PRIVACY

No specific information has been provided as to what data is stored on the devices or on the backend, though based on the limited disclosures, certain data can.

be inferred to be collected. Based on images and description on Estimote's website, it appears that an employee's movements, proximity (and duration) to other employees, and actual (or believed) infection is collected and stored by the backend. The movement and proximity data is likely to be stored by the device before being transmitted to the backend. It is known whether the employee's personal information is stored on the device, or in the backend, or both. It also appears that specific location within the company can be collected if used in conjunction with out Estimote beacon technology, or via the limited indoor GPS capabilities of the device.

While Estimote believes that employees should opt-in, there is no stated method for obtaining consent. The Estimote Terms of Service state that the company is responsible for obtaining the necessary rights from the employee, but there are no specifics as to the scope of consent required. Further, as noted above, the Terms of Service are from 2015 and do not address wearable devices, nor GDPR requirements.

Under the GDPR, data subjects have the right to access information being processed about him or her and may request correction or deletion of their data under certain circumstances, however, there is no information disclosed about how this will work either with Estimote or the implementing companies. Estimote appears to view itself as acting as a processor, though the language of its documentation make that less than fully clear. Estimote appears to be relying on its customers (the implementing companies) to have determined the lawful basis for processing, and states in its Privacy Policy that "Customer Data Is owned and controlled by our customers...we collect and process Customer Data solely on behalf of our customers...." There do not appear to be any requirements on control of data.

There is no information available regarding security processes, de-identification, or anonymization of the information to be collected and stored by the implementing companies, nor by Estimote.

CONCLUSION

The Estimote solutions presents several high risks largely due to the lack of information and disclosures about the solution. While employees may benefit from a solution that helps them stay safe and healthy, it is unknown whether the Estimote solution will, in fact, do so. There is no information on the majority of the principles set forth in the PIA. This includes information as to the serious privacy, cybersecurity and related concerns that the technology raises, as well as analysis of the potential legal and regulatory requirements, such as those under privacy and data protection laws and regulations (i.e., GDPR, CCPA, PIPEDA), workplace monitoring and safety laws and regulations, laws against discrimination, telecommunications regulations, collective bargaining agreements, regulations for wearable devices, regulations for medical devices, and protections from mass surveillance.

The centralized solution presents a weak point which is further exacerbated by the apparently lack of standards on implementations. While some implementing companies may have rigorous security, need to know disclosures, and opt-in participation, there will likely also be companies that don't. If the central server is compromised, the entire system would then likely be compromised, including employee health and location data. However, in order for the solution to be effective, employees should opt-in, yet doing so gives up virtually all of their autonomy and control over their own data.

Lastly, the reliability of the solution is also unknown. If the devices malfunction, it could put employees and potentially the company's customers at risk.

TerraHub
Credential Link PostCoviData Impact Assessment ("PIA") Overarching Risk Summary (Key Findings)

May 26, 2020

by Adrien Basdevant, Caroline Leroy-Blanvillain (Basdevant Avocats, France)

To be read in conjunction with main PIA for TerraHub Credential Link Solution, dated 26 May 2020.

FACTORS JUSTIFYING NEED FOR IMPACT ASSESSMENT

TerraHub has developed a verification platform for workers, products, and processes. The company's product, Credential Link builds an irrefutable audit trail for worker training, authorizations, and health self-assessments. It thus provides workforce management tools for verifying and sharing health self-assessments, safety and professional certificates. In the early days of COVID-19, TerraHub recognized that its Credential Link solution might have a role in controlling the spread of the virus. On this platform, employers have access to critical worker information before they arrive on site. Accordingly, employees are now able to upload for example COVID-19 test results or training courses relating to sanitary measures.

Each individual has the following data associated with them: personal identity information, credential details, credential verification details, audit trail history, employer and project associated details. The total volume of data for each individual is under 500Kb (average). However, aggregate data for analytics is spread across an entire organization's user base. So, organizations can have a relatively large amount of data to work with to make decisions based on analytic data.

Three stakeholders were identified: the organization deploying the tool (i.e the employer), the workers using the tool (i.e the employees) and the organizations issuing the credentials (i.e the issuers). The Solution works with the Hyperledger Fabric blockchain protocol. Each individual is authenticated using a public key that is registered when the individual is given access to the relevant shared private channel. The data cannot be read nor updated by any individual not previously registered. There are two kind of access: user access and admin access. Admin access is limited to authorized roles from the employer. Specific symptoms reported by the worker can only be accessed by that worker. Employer gets an OK/Not OK summary for each worker without any detailed elements relating to the self-assessment. Data may be shared with the third parties by giving explicit consent and access can be revoked by the worker. Third parties are the organizations to which the worker gives the authorization to access the data.

This update of the solution has been released in April 2020 to help companies ensure the safety of employees returning to work after the lockdown period. The main ethical concerns may relate to the following points:

- Whether the blockchain-based technology used allows the users to effectively exercise their rights (re modification / erasure) ;
- Whether both the technology used, and the algorithm added for the health self-assessment are transparent and explainable ;
- Whether the use of Credential Link by the employer might affect the rights and interests of employees, for example by creating discriminatory situations ;
- Whether the governance of the solution clearly frames the secondary use of data inferred from the solution by the employer.

A supplemental PIA is useful in the context of the implementation of the Pandemic Tech Solution to exit the sanitary crisis and help secure workplaces. Indeed, the relationship between employer and

employees is deemed to be unbalanced per se, and accordingly it should be assessed whether the use of this Solution by the employer may threaten the rights and interests of the employee.

More specifically, three ethical concerns have been identified at this point:

- How to ethically frame the decisions taken by the employer when receiving a "NOT OK" summary from the Solution ?
  - For example, might a "NOT OK" worker obliged to stay home suffer from a salary loss or a red flag in its relating personnel file ?
  - Also, what would happen in a given organization, if an employee refuses to use this solution ?
  - How does the "OK/NOT OK" summary is completed ? Can we infer information from this summary ?
- How to ensure that the employee will not overpass or lie on the self-assessment to avoid any repressive action from the employer ?
  - For example, might an employee afraid of repressive action lie on the self-assessment health status and thus render the Solution inefficient by putting at risk other workers of the company ?
  - NB: The irrefutable nature of a blockchain technology is useful if and only if the primary source of information is reliable.
- Are there any ways to use this data by the employers for different purposes initially planned ?
  - Is the data provided by the employee stored on-chain or off-chain ?
  - Is there a way for employer to store a copy of this data ? (e.g screen shots)

Additionally, the Solution collects and displays to the employer sensitive data, for which it must be ensure maintaining security and integrity as well as preserving a certain control from the employees.

This PIA should help both TerraHub and Project Owner to deploy the Solution with respect to legal and ethical principles to trade-off between organization's interests of workplace safety and rights and privacy of workers.

It should be noted that part of the assessment leading to the issue of the OK/NOT OK summary is based on a simple algorithm (i.e. for the health self-assessment) that is not deemed to integrate AI or machine-learning as defined in the present Pandemic Impact Assessment framework. However, such completion should be considered if complementary information about the functioning of the algorithm could indicate otherwise.

PRINCIPLE 1 – ETHICAL PURPOSE & SOCIETAL BENEFIT

The solution is currently deployed in Canada only, but might completely be deployed in other regions/ countries which could significantly modify the risk rating relating to the legal framework. The relevance and proportionality of the use of Credential Link should be assessed by the Project Owner with regard to the excessive surveillance of employees that it may engender.

Furthermore, while deploying this solution, it should particularly be assessed who will be subject to the use of the solution (i.e. only employees or any person entering a site of the Project Owner) and how the data will be use to limit any infringement to the rights of users.

High risks were also identified regarding the use of the Summary by the employer, which might significantly affect the autonomy of workers and thus should be carefully framed. The Project Owner should consider not to take decisions significantly affecting the autonomy and / or dignity of workers on the sole basis of the solution at stake.

Finally, considering that information about credentials and self-assessments is stored off-chain, it partially prevents the data from being publicly available in an irrevocable manner. Accordingly, it remains the responsibility of each issuer to implement appropriate safeguards including time-limit or automatic deletion of the information. However, it should be noted that the worker can revoke the authorizations granted to access the data, which appears as a minimum appropriate safeguard as well.

PRINCIPLE 2 – ACCOUNTABILITY

Centralized and decentralized components should be detailed, regarding both the protocol and/or the governance of the solution. Accordingly, the governance of Credential Link should be determined precisely by the Project Owner, as it is the first step to rate the level of risk inherent to the implementation of the solution. Some measures were taken by TerraHub to limit the technical and privacy risks, nonetheless it will also depend on the way the organization will deploy and implement Credential Link.

Also, sufficient measures should be implemented to determine if the decision-making process allows Project Owner operators to adjust parameters, to follow or not the Summary output, etc.

Data is stored both on and off chain. Off chain data require encryption and a distributed model uses QLDB ; off chain data requires encryption stored in S3. On chain, are only stored the hashes that point to all the off-chain sources so as to ensure no changes are made off-chain. All "issuers" are identified by the network as the originators of a credential. Employer can define an administrator that can access public employee information, for example credentials, but not health self-assessments. An employer can be an "issuer" and a "reader", and they can define an administrator that can access public employee information, for example credentials, but not health self-assessments.

The Project Owner should ensure at all time it remains accountable for the responsible deployment of the Solution, including by means of “human-in-the-loop” or “human-over-the-loop” to make sure that humans oversight is active and involved in relation to recommendation provided by the “OK/NOT OK” Summary.

PRINCIPLE 3 – TRANSPARENCY AND EXPLAINABILITY

Two issues must be distinguished when assessing transparency and explainability criteria for Credential Link: the permissioned blockchain protocol, on the one hand, and the private algorithmic decision making tool, on the other hand. Indeed, regarding the health self-assessment, an algorithm is implemented in the solution to assess whether a worker presents risks of exposure to COVID-19. This algorithm consists in a basic survey on the employee’s latest actions deemed to be “at-risk” (e.g. traveling, symptoms, contact with infected person). Considering that no access was given to the survey nor the algorithm itself, it is not possible to determine the risk rating of obtaining a false summary. Nor it is possible to determine if the outputs of the algorithms could be explained or if the functioning of the algorithm could be explained (black-box situation). It is assumed that the use of such a basic algorithm contributes to limiting this risk but does not eliminate it completely as false positives or false negatives are still possible, thus questioning the transparency of the application. As far as the blockchain protocol is concerned, in

order to limit the risks regarding explainability, the Project Owner should take appropriate measure to make sure that such innovative and complex technology is being fully understood by its users.

Moreover, it seems that very few materials are currently available to users, which may identify a mitigation measure to be taken. The functioning of the solution should be explained to employees, with all the consequences attached to the use of that solution. No opacity should remain on the conditions of use, the privacy issues, and how the solution works.

PRINCIPLE 4 – FAIRNESS & NON-DISCRIMINATION

The data processed by Credential Link is only modified but not transformed, or only to the extent of providing the Project Owner with the summary but in that case, only the granularity of available data changes.

Besides, inequalities inherent to the use of the application may arise between workers familiar with technologies and the ones for whom the use of blockchain technology means very little. More precisely, if the use of Credential Link is not mandatory but voluntary or incentive, it should be assessed whether all workers will be able to acknowledge all the outputs of accepting to use it. This can relate to the idea of an "ethically" free and informed consent. Indeed, such a consent to use the app may be guided by employer pressure, or social pressure, for example if there are beneficence or maleficence effects attached to the use of Credential Link, which could appear infringing the fairness principle.

Finally, the risk of having derivative misuse of the application appears high if no conditions are clearly set while implementing it.

PRINCIPLE 5 – SAFETY AND RELIABILITY

It appears that TerraHub implemented strong technical and organizational measures to ensure both safety and confidentiality of the Pandemic Tech Solution, by adopting recognized technical standards including encryption all along the transactions. The most pregnant risk remaining relates to the redress mechanisms, for example in case of hacking resulting in the loss of the credentials, as no information has been provided on that point.

The blockchain technology used lowers the risk of falsification, once the hash of the data is stored on-chain, but could not guarantee that the original source of the data stored off-chain is reliable.

However, the risk of dual use is assumed to be high, as once the Project Owner has the lead on the solution and collect inferred data, it becomes difficult to control any subversion of intended use.

PRINCIPLE 6 – OPEN DATA, FAIR COMPETITION & INTELLECTUAL PROPERTY

The fact that Credential Link relies on an open source blockchain protocol increases transparency and prevent from most of infringement risks to intellectual property rights.

More generally, when assessing such a solution working with a blockchain protocol and a algorithm layer, this Principle should be assessed with regards to each part of the solution, as the analysis may vary considering the blockchain protocol (here open-source) or the algorithm (here proprietary and non-public).

PRINCIPLE 7 – PRIVACY

There is often a warning to be issued when employer / employee relationship is at the core of the use of a technology. In the present case, there might be risks regarding the preservation of workers' privacy, which TerraHub has tried to limit at best to only grant access to the minimum information required. The employee keeps control over the provided data, both with the authorization system and the possibility to disactivate the application.

Nevertheless, risks remain regarding the use by the employer / Project Owner of the information extracted from Credential Link. The major concern with this solution was about the information being stored on-chain, which would have resulted in the impossibility to exercize the rights of correction and/or erasure thus severely affecting the rights of workers. It appears that workers' data is stored off-chain and is accordingly not publicly available, and consequently the retention period and deletion

of the data remain of the sole responsibility of the organizations storing it.

It should also be noted that regarding specifically the answers to the health self-assessment, the worker cannot modify them anymore once submitted, but can re-take the survey. The Project Owner should assess whether appropriate safeguards are implemented regarding the rights to privacy of workers, notably by determining efficient processes for employees to exercise their rights.

If Privacy and Data Protection concerns remain reasonable regarding the design of Credential Link, further risks appear when considering secondary use of the data by Project Owner. More specifically, it is here considered the possibility for Project Owner to process any derived or inferred data collected from the summary or any other feature provided by the solution. Such a use could entail severe consequences for the workers and should be consciously framed when deploying Credential Link within an organization.

CONCLUSION

The Credential Link solution seems to offer some safeguards to reach its purpose: ensuring a safe return to work for organizations adopting it. However, two kinds of risks should be particularly observed: i) risks inherent to the design of the solution itself, and ii) risks linked to the implementation of the solution by the Project Owner.

Regarding the risks inherent to the solution itself, the present Pandemic Impact Assessment reveals that the worker data is at least stored off-chain, which limits the risk of rending the data constantly and publicly available on the blockchain. The fact that data is stored off-chain results in the transfer of responsibility to the organization by which the data is stored for implementing appropriate retention period and erasure processes, with respect to the principle of data minimization that could lead the choice of adopting a Pandemic Tech Solution. Besides, the Project Owner should in either way ensure that any organization accessing the worker's data, or processing derived or inferred data, implemented adequate retention periods and processes for workers to effectively exercise their rights, thus making sure for the end-user that all the information will eventually be deleted from systems of third parties to which s.he granted authorization at once. It should also be highlighted that the use of blockchain, if it allows to have irrefutable and accurate data, also entails the impossibility to verify the veracity of the updated data

Furthermore, regarding the specific question of the summary made available to the employer, it should be noted that the health self-assessment is based on a simple algorithm: it determines if a worker is OK by tallying the answers and indicating OK if the person has no symptoms, has not travelled or come into contact with a sick person. Once the answers are submitted, the worker cannot modify the answers, but can take the survey again. Therefore, it should be assessed the possibility for the employer to access the previous results of the assessment or whether only the latest results are displayed which could contain a risk of falsification if the worker takes the test again to artificially modify the result. However, the possibility for the employer to access the previous results would potentially infringe the principles of necessity, proportionality, and data minimization. Consequently, arises a trade-off between privacy preservation and workers' protection on the one hand, and the need for accuracy on the other hand.

Another identified risk is the lack of documentation available for the end-user. Due to the context in which the assessment was led, maybe this documentation has just not come to our attention, but it seems that no Terms of Use or Privacy Policy is available for the solution. Terms of Use appear to be of crucial importance, as the use of Credential Link by employers may have significant consequence on employees in case of misuse (both by the employee in case of lie and by the employer in case of disrespectful secondary use).

CONCLUSION (CONT'D)

Regarding the risks inherent to the adoption of the solution by the Project Owner, more significant concerns should be raised. First, the consequences of the summary sent to the employer should be precisely determined and discussed prior to the adoption of the solution, to prevent any infringement to the rights of employer and any discriminatory measures. For example, if the daily summary indicates that the worker is “NOT OK” (i.e. s.he cannot access the workplace without putting at risk its coworkers), there should be a procedure indicating if the worker shall stay home, but it should also be documented what it implies concretely. More precisely, it could be imagined that if the worker is in incapacity of accessing safely the workplace because s.he does not hold verified COVID-19 testing results, it will entail a loss of salary corresponding to the time spent home, which might be deemed as a discriminatory measure as if the solution had not been implemented, the employee would not have suffered such a loss.

The other major risk in the context of implementation of the solution relates to the secondary use of the data made by the Project Owner. While considering adopting a Pandemic Tech Solution as Credential Link, it should be assessed to what extent analytics or secondary use of the collected data may be done. This point partially relates to the previous one as secondary use should be determined to avoid any use against the employee and making sure there will be no misusage leading to discriminatory situation, whether by comparing the data from a particular worker to another or by using the data to make decision that would not benefit the workers and that would not have been taken without access to this data.

Mitigation measures should integrate a specific internal body ensuring to respect the rights of workers while thinking of the implementation of Credential Link.


Bitte halten
Sie Abstand!

BIBLIOGRAPHY

REPORTS, DECLARATIONS

1. Atlantic Council, *COVID-19's potential impact on global technology and data innovation*, April 13, 2020. https://atlanticcouncil.org/blogs/geotech-cues/COVID-19s-potential-impact-on-global-technology-and-data-innovation/ (consulted on May 13, 2020).
2. Académie des Sciences, *COVID-19 pour une surveillance basée sur le volontariat*, https://www.academie-sciences.fr/pdf/rapport/2020_04_10_avis_tracage.pdf (consulted on May 13, 2020)
3. J. Bay, "Automated contact tracing is not a coronavirus panacea", *Government Digital Service - Singapore*, https://blog.gds-gov.tech/automated-contact-tracing-is-not-a-coronavirus-panacea-57fb3ce61d98 (consulted on May 13, 2020).
4. Comité Consultatif National d'Ethique, *La contribution du CCNE à la lutte contre COVID-19 : Enjeux éthiques face à une pandémie*, https://www.ccne-ethique.fr/fr/publications/la-contribution-du-ccne-la-lutte-contre-COVID-19-enjeux-ethiques-face-une-pandemie (consulted on May 13, 2020).
5. Comité national pilote d'éthique du numérique, *Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aiguë*, https://www.ccne-ethique.fr/sites/default/files/publications/bulletin-1-ethique-du-numerique-covid19-2020-04-07.pdf, (consulted on May 13, 2020)
6. Commission de l'éthique en science et en technologie, "Enjeux éthiques liés à la pandémie de COVID-19", https://www.ethique.gouv.qc.ca/fr/publications/ethique-covid19/ (consulted on May 13, 2020).
7. Council of Europe, *Modernisation of the Data Protection "Convention 108"*. https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet (consulted on May 31, 2020).
8. Council of Europe, *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf (consulted on May 31, 2020).
9. Council of Europe, Committee of Ministers, *Algorithms and automation: new guidelines to prevent human rights breaches*, https://www.coe.int/en/web/cm/news/-/asset_publisher/hwwluK1RCEJo/content/algorithms-and-automation-new-guidelines-to-prevent-human-rights-breaches/16695 (consulted on May 31, 2020).
10. Datenschutz, *Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie*. https://www.datenschutzkonferenz-online.de/media/en/Entschlie%C3%9Fung%20Pandemie%2003_04_2020_final.pdf, (consulted on May 2020)
11. *Montréal Declaration for a Responsible Development of Artificial Intelligence*, https://www.declarationmontreal-iaresponsable.com (consulted on May 13, 2020).
12. European Commission, *Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*. https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf, (consulted on May 31, 2020)
13. European Commission, "Coronavirus: An EU approach for efficient contact tracing apps to support gradual lifting of confinement measures", *Shaping Europe's digital future*, avr. 16, 2020. https://ec.europa.eu/digital-single-market/en/news/coronavirus-eu-approach-efficient-contact-tracing-apps-support-gradual-lifting-confinement (consulted on May 31, 2020)
14. European Data Protection Board, *Statement on the processing of personal data in the context of the COVID-19 outbreak*, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandCOVID-19_en.pdf, (consulted on May 31, 2020)
15. European Data Protection Supervisor, *Monitoring spread of COVID-19*, https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_COVID-19_monitoring_of_spread_en.pdf, (consulted on May 31, 2020)
16. International Federation for Human Rights, *"COVID-19 - Prioritise human rights and protect the most vulnerables"*, https://www.fidh.org/en/issues/human-rights-defenders/COVID-19-prioritise-human-rights-and-protect-the-most-vulnerable (consulted on May 13, 2020).
17. Future of privacy Forum, *Artificial Intelligence and the COVID-19 Pandemic*, https://fpf.org/2020/05/07/artificial-intelligence-and-the-COVID-19-pandemic/ (consulted on May 13, 2020).
18. "G20 Trade and Digital Economy Ministers adopt statement in Tsukuba", *Trade - European Commission*. https://trade.ec.europa.eu/doclib/press/index. cfm?id=2027 (consulted on May 31, 2020).
19. Information Commissioner's Office, *Data protection impact assessments*, April 15, 2020. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/ (consulted on May 31, 2020).
20. Information Commissioner's Office, *Sample DPIA template*, https://iapp.org/media/pdf/resource_center/dpia-template-v04-post-comms-review-20180308.pdf, (consulted on May 31, 2020)
21. ITechLaw, *Responsible AI: A Global Policy Framework*, June 14, 2019. https://www.itechlaw.org/ResponsibleAI (consulted on May 31, 2020)
22. M., Mahjoubi , *Note parlementaire Version 1.0 du lundi 6 avril 20*, http://d.mounirmahjoubi.fr/TracageDonneesMobilesCovidV1.pdf, (consulted on May 13, 2020)
23. McKinsey, *Contact tracing for COVID-19: New considerations for its practical application*, https://www.mckinsey.com/industries/public-sector/our-insights/contact-tracing-for-COVID-19-new-considerations-for-its-practical-application?cid=other-eml-alt-mip-mck&hlkid=828ba682899043c9b4626cffc6748619&hctky=2723747&hdpid=c8873e56-2263-4a01-b712-ccf574693275 (consulted on May 13, 2020).
24. A. Olbrechts, " *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak ", Comité Européen de la Protection des Données - European Data Protection Board*, April 22, 2020. https://edpb.europa.eu/our- work-tools/our-documents/usmernenia/guidelines-042020-use-location-data-and-contact-tracing_fr (consulted on May 13, 2020).
25. *PEPP-PT Pan European Privacy Protecting Proximity Tracing*, https://404a7c52-a26b-421d-a6c6-96c63f2a159a.filesusr.com/ugd/159fc3_878909ad0691448695346b128c6c9302.pdf, (consulted on May 31, 2020)
26. Personal Data Protection Commission - Singapore, *Model artificial intelligence governance framework*, https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf, (consulted on May 31, 2020)
27. US Federal Trade Commission, *Using Artificial Intelligence and Algorithms*, avr. 08, 2020. https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms (consulted on May 31, 2020).
28. World Economic Forum, *Gig workers among the hardest hit by coronavirus pandemic*, https://www.weforum.org/agenda/2020/04/gig-workers-hardest-hit-coronavirus-pandemic/ (consulted on May 25, 2020).

ACADEMIC REFERENCES

29. Ada Lovelace Institute, *COVID-19 Rapid Evidence Review: Exit through the App Store?*, https://www.adalovelaceinstitute.org/our-work/COVID-19/COVID-19-exit-through-the-app-store/ (consulted on May 13, 2020).
30. C. Batut et A. Garnero, "L'impact du COVID-19 sur le monde du travail : télémigration, rélocalisation, environnement", *Le Grand Continent*, https://legrandcontinent.eu/fr/2020/05/01/limpact-du-COVID-19-sur-le-monde-du-travail-telemigration-relocalisation-environnement/, (consulted on May 31, 2020)
31. A. Casilli, *En attendant les robots*. Le Seuil, 2019.
32. X. Bonnetain, A. Canteaut, V. Cortier, P. Gaudry, L. Hirschi, S. Kremer, S. Lacour, M. Lequesne, G. Leurent, L. Perrin, A. Schrottenloher, E. Thomé, S. Vaudenay, C. Vuillot, *Le traçage anonyme, dangereux oxymore. Analyse de risques à destination des non-spécialistes*, https://risques-tracage.fr/docs/risques-tracage.pdf, (consulted on May 13, 2020)
33. M. Foucault, Surveiller et punir. *Naissance de la prison*. Editions Gallimard, 2014.
34. Le Centre de recherche en éthique, *Les enjeux éthiques des applications anti-pandémie*, http://www.lecre.umontreal.ca/les-enjeux-ethiques-des-applications-anti-pandemie/ (consulted on May 13, 2020).
35. E. Lemonne, "Ethics Guidelines for Trustworthy AI", FUTURIUM - *European Commission*, déc. 17, 2018. https://ec.europa.eu/futurium/en/ai-alliance-consultation (consulted on May 31, 2020).
36. Leopoldina, Nationale Akademie der Wissenschaften, *Coronavirus-Pandemie – Die Krise nachhaltig überwinden*, https://www.leopoldina.org/publikationen/detailansicht/publication/coronavirus-pandemie-die-krise-nachhaltig-ueberwinden-13-april-2020/ (consulted on May 31, 2020).
37. D. Rotman, "COVID-19 has blown apart the myth of Silicon Valley innovation", *MIT Technology Review*, https://www.technologyreview.com/2020/04/25/1000563/COVID-19-has-killed-the-myth-of-silicon-valley-innovation/ (consulted on May 13, 2020).
38. B. Sportisse, "Contact tracing", *Inria*, https://www.inria.fr/fr/contact-tracing-bruno-sportisse-pdg-dinria-donne-quelques-elements-pour-mieux-comprendre-les-enjeux (consulted on May 13, 2020).
39. J. Stanley, J. S.Granick, "The Limits of Location Tracking in an Epidemic", *American Civil Liberties Union*, https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf, (consulted on May 13, 2020)

PRESS, MEDIAS

40. "Individual vs Group Privacy", *IThappens.nu*, mars 20, 2019. http://www.ithappens.nu/individual-vs-group-privacy/ (consulted on May 31, 2020).
41. J. Dingel et B. Neiman, "How many jobs can be done at home?", *VoxEU.org*, avr. 07, 2020. https://voxeu.org/article/how-many-jobs-can-be-done-home (consulted on May 25, 2020).
42. D. Gershgorn, "We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World", *OneZero*, https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9 (consulted on May 13, 2020).
43. H. Guillaud, "StopCovid : le double risque de la "signose" et du "glissement"", *Medium*, https://medium.com/@hubertguillaud/stopcovid-le-double-risque-de-la-signose-et-du-glissement-b1e2205bff5a (consulted on May 13, 2020).
44. A. Marty, "Ce que L'automatisation visuelle apportera au monde Post-COVID-19", *Forbes France*, mai 04, 2020. https://www.forbes.fr/technologie/ce-que-lautomatisation-visuelle-apportera-au-monde-post-COVID-19/ (consulted on May 25, 2020).
45. E. Massé, "Privacy and public health: the dos and don'ts for COVID-19 contact tracing apps", *Access Now*, https://www.accessnow.org/privacy-and-public-health-the-dos-and-donts-for-COVID-19-contact-tracing-apps/ (consulted on May 13, 2020)
46. E. Morin, "Nous devons vivre avec l'incertitude", *CNRS Le journal*. https://lejournal.cnrs.fr/articles/edgar-morin-nous-devons-vivre-avec-lincertitude (consulted on May 13, 2020).
47. F. Saadi, "COVID-19 et retail : un nouveau fonctionnement s'impose pour les distributeurs", *L'Usine Digitale*, https://www.usine-digitale.fr/article/COVID-19-et-retail-un-nouveau-fonctionnement-s-impose-pour-les-distributeurs.N961681 (consulted on May 25, 2020)

CONTRIBUTORS

STEERING COMMITTEE

Jean-Louis Davet
President
Denos Health Management
Paris

David Doat
Senior Lecturer, Philosophy
Université catholique de Lille
(Laboratoire ETHICS)
Lille

Marie Élaine Farley
CEO
Chambre de la Sécurité
Financière
Montréal

Anne-Marie Hubert
EY, Managing Partner
Human Technlology Foundation,
President
Montréal

Nathalie de Marcellis-Warin
CIRANO, CEO
Polytechnique Montréal / OBVIA,
Full Professor
Montréal

Charles S. Morgan
International Law Association,
President
McCarthy Tétrault LLP, Partner
Montréal

Eric Salobir
President
Human Technology Foundation
Paris

PROJECT LEAD

Adrien Basdevant
Founding Lawyer
Basdevant Avocats
Paris

Caroline Leroy-Blanvillain
Lawyer
Basdevant Avocats
Paris

HUMAN TECHNOLOGY FOUNDATION

ANALYST

Pierre Gueydier
Directeur de la recherche
Human Technology Foundation
Paris

COMMUNICATION

Antoine Glauzy
General director
Human Technology Foundation
Montréal

Sibylle Tard
Lead, Lab.222
Human Technology Foundation
Paris

ETHICS TEAM

Allison Marchildon
Associate Professor
Université de Sherbrooke / OBVIA
Montréal

Manuel Morales
Associate Professor
Université de Montréal / Fin-ML
Network / OBVIA
Montréal

Yves Poullet
Université de Namur / Université
Catholique de Lille (ETHICS)
Honorary Rector, Université de
Namur, Associate Professor
Université Catholique de Lille
Namur

Bryn Williams-Jones
Full Professor
École de Santé Publique de
l'Université de Montréal / OBVIA
Montréal

LEGAL TEAM (ITECHLAW ASSOCIATION)

Belén Arribas Sanchez
Partner
Andersen Tax & Legal
Barcelona

Edoardo Bardelli
Trainee lawyer
Gattai, Minoli, Agostinelli &
Partners
Milan

John Buyers
Partner
Osborne Clarke LLP
London

Philip Catania
Partner
Corrs Chambers Westgarth
Melbourne

Ellen Chen
Associate
McCarthy Tétrault LLP
Montréal

Massimo Donna
Managing Partner
Paradigma Law
Milan

Licia Garotti
Partner
Gattai, Minoli, Agostinelli &
Partners
Milan

Marco Galli
Senior Associate
Gattai, Minoli, Agostinelli &
Partners
Milan

Doron S. Goldstein
Partner
Katten Muchin Rosenman LLP
New York City

Dean W. Harvey
Partner
Perkins Coie LLP
Dallas

Lara Herborg Olafsdottir
Partner
Lex Law Offices
Reykjavik

Charles-Alexandre Jobin
Associate
McCarthy Tétrault LLP
Montréal

Jenna F. Karadbil
Founder
Law Office of Jenna F. Karadbil, P.C
New York City

Rheia Khalaf
Director
University of Montreal
Collaborative Research &
Partnerships *Fin-ML/IVADO*
Montréal

Aparajita Lath
Associate
Trilegal
Bangalore

Kit Mun Lee
Associate
Corrs Chambers Westgarth
Melbourne

Swati Muthukumar
Associate
Trilegal
Bangalore

Nikhil Narendran
Partner
Trilegal
Bangalore

Smriti Parsheera
Fellow
CyberBRICS Project
New Delhi

Patricia Shaw
CEO
Beyond Reach Consulting Limited
London

Alexander Tribess
Rechtsanwalt Partner
Weitnauer Partnerschaft mbB
Hamburg

Padraig Liam Walsh
Partner
Tanner De Witt Solicitors
Hong Kong

Alan Wong
Registered foreign lawyer –
Solicitor
Tanner De Witt Solicitors
Hong Kong

TECHNICAL TEAM

Victor de Castro
Chief Medical Officer
Philips Health Systems
Paris

Maxime Fudym
Developer
Waxym
Paris

Roberto Mauro
Managing Director Europe,
Strategy & Innovation Center
Samsung Electronics

Gilles Mazars
Director of Engineering –
Advanced Innovation Lab
Samsung Electronics
Paris

Pascal Voitot
Samsung Electronics
Applied Research Scientist
in Deep/Machine Learning –
Advanced Innovation Lab
Paris

Jean-Jacques Wacksman
Developer
Waxym
Paris

MANY THANKS TO OUR PARTNERS


Sector 2
Sector 3