Journal of Law, Technology and Trust, Vol 1, Issue 1, 2020

Privacy as Public Good – A Comparative Assessment of the Challenge for CoronApps in Latin America

Kim Barker, Enrique Uribe-Jongbloed, Tobias Scholz

Abstract

Much of the reporting of the tracing apps, tracking programmes, and privacy concerns during the developmental processes and the initial stages of the Covid-19 pandemic have focussed on pitting digital rights and privacy against public health interests. Undoubtedly, there is best practice in establishing a tracing app to respond to Covid-19 while the work of civil society and NGOs in scrutinising the apps in various nations is vitally important and provides the core analysis of the scope of the data to be collated and retained. The holding to account of tracing systems and governments in utilising technology that is by its very nature invasive is vital in protecting digital rights. In times of crisis in particular, accountability is incredibly important to ensure that digital rights are not pushed aside in light of other concerns.

To balance digital rights and privacy, and public health, accountability and transparency are essential – the scrutiny of the track and trace systems in Germany, the UK, and Colombia is therefore undertaken in this paper, which questions from interdisciplinary perspectives the scrutiny, accountability, and privacy concerns in each nation's app before offering some conclusions and recommendations for the improvement and development of privacy and digital rights in Latin America. The conclusions offered here highlight good practice and outline the need for a holistic consideration of tracing systems, rather than advocating for a 'one size fits all approach' by positioning privacy as a public good, rather than an opponent of technological tracing systems.

Keywords: CoronApp, Latin America, Europe, Privacy

1. Introduction

The Covid-19 pandemic has not caused new issues[1] in respect of dealing with personal data, privacy, and technological regulation but has, instead, given a renewed prevalence to issues relating to information sharing and the collating of data. The conflict between the need for information and privacy – especially in a health context – has risen exponentially in 2020 as part of the response to the pandemic. Tensions in this area have come to the fore through the unveiling of so-called 'corona-apps' to allow track and trace programmes to operate as part of a more holistic public health approach to measuring and controlling outbreaks of Covid-19.

With the rise and spread of infection, there has been a parallel rise in track and trace apps, all handled slightly differently across different national borders. Within these divergent approaches, common challenges arise – notably how to collect data to inform the public health response to the pandemic, whilst also ensuring that the apps are fit for purpose, widely used, and do not collect data unnecessarily. The unique package of the pandemic, together with the clash of rights and regulatory priorities provides an opportunity to undertake a comparative analysis of limitations to privacy and data protection in Latin America and beyond. This paper therefore undertakes such an analysis, and in doing so, fills that knowledge gap.

In this article we present the risks of unaccountable data collection that have arisen during the times of Covid-19 in Colombia and Ecuador. We analyze the Colombian "CoronApp" issued by the Instituto Nacional de Salud – INS – (Institute of National Health) on the 7 of March, 2020[2] as well as "Salud EC" in Ecuador alongside others from Germany, and the UK,[3] all of which are aimed at capturing information that would help to track and trace the spread of the Covid-19 virus. In comparing the successes of the various tracing apps, this paper will explore the utility such apps have shown in containing the pandemic[4] in spite of the serious concerns about privacy violations. In order to analyze the Colombian and – to a lesser extent –

---

[1] In some states, data protection regulations can be set aside in times of crisis, raising concerns about the suitability of protections for personal information even in unforeseen situations such as COVID-19. See: Morgan Lewis, 'Coronavirus v. GDPR: Suspending Data Privacy Protection During Civil Crisis – The eData Guide to GDPR' (*JD Supra*, 10 March 2020) <https://www.jdsupra.com/legalnews/coronavirus-v-gdpr-suspending-data-85584/> accessed 22 July 2020.

[2] Ministry of Health, 'CoronApp – Colombia, the application to know the evolution of the coronavirus in the country' (*Ministry of Health*, 7 March 2020) <https://www.minsalud.gov.co/Paginas/CoronApp.aspx> accessed 22 July 2020.

[3] Yadira Trujillo, 'Gobierno de Ecuador presenta la 'app' Salud EC para acceder a una evaluación del covid-19 y recibir información' (*El Comercio*, 25 March 2020) <https://www.elcomercio.com/actualidad/coronavirus-app-salud-ecuador-telemedicina.html> (accessed 22 July 2020).

[4] William Hicks, 'Thai Covid-19 apps judged invasive' (*Bangkok Post,* 20 July 2020) <https://www.bangkokpost.com/business/1954287/thai-covid-19-apps-judged-invasive> accessed 22 July 2020.

Ecuadorian examples in Latin America,[5] we start by reviewing the German and UK examples, to see how those nations confronted the issue. We then draw from them lessons for analyzing the Colombian and Ecuadorian application and forms, and for assessing the privacy framework in Latin America in respect of the evolving norm of privacy as a public good.

These jurisdictions have been selected because of the differences in responding to the Covid-19 pandemic, but also the different regional responses. In selecting Germany and the UK, and Colombia and Ecuador as examples, two examples are taken from two continental regions (Europe, and Latin America) to enable a comparison of responses seen through the perspectives of culture, data protection, and media reporting. The comparisons made in this paper represent a number of perspectives, including analysis of organizational national cultures, as presented by Hofstede, Hofstede and Minkov,[6] a legal analysis of the data protection developments in the countries, and media perspectives on how this issue has been publicly debated. From the first perspective, Latin American cultures (such as Colombia and Ecuador) are deemed to present higher power distance (more respect and value for authoritarianism and following a strong leader, for instance) and lower individualistic values (fostering more consensus and valuing the collective more than the individual), in comparison to their European counterparts. That is particularly relevant when in legislation on privacy in Latin America,

> in formal terms, there is a tendency for the need for the inviolability, protection and respect for privacy to be underscored; [yet] on the other hand, the cultural dimensions related to the tolerance of unequal relations of power and an undervalue of individuality, tend to blur the person and their rights. In this sense, there is a legal dynamic that tries to keep the sacred value of the person, through legal frames that protect privacy and personal data, but in a context that disregards it constantly.[7]

A situation such as the current Covid-19 pandemic presents itself as an interesting case in point because it provides a scenario in which to study both the cultural aspects behind the actions undertaken by the national or local leaders and the extent to which privacy, data protection, regulation, and social constructions of control are followed or debated in the public sphere. In particular, through the various Apps developed in Colombia and Ecuador to address the Covid-19 threat, it is possible to

---

[5] These are not the only Latin American states where issues surrounding Corona-Apps are problematic – a similar app in Chile has also been subjected to scrutiny given the absence of adequate data protections. See: International Law Firm Alliance, 'The legal implications of Contact Tracing in Chile' (*Abdala & CIA Abogados,* 29 May 2020) <https://diazreus.com/wp-content/uploads/2020/06/LATAM_contact-tracing.pdf> accessed 22 July 2020.

[6] Geert Hofstede, Gert Jan Hofstede and Michael Minkov, *Cultures and Organizations: Software of the Mind* (McGraw-Hill 2010).

[7] Nelson Arteaga and Liliana Onofre, 'La protección a la privacidad en América Latina' in Karina Ansolabehere, Francisco Valdés Ugalde & Daniel Vásquez (eds) *Entre el pesimismo y la esperanza: Los derechos humanos en América Latina.Metodología para su estudio y medición* (FLACSO-México 2015), 384. Authors own translation

see how governments in Latin America have confronted – or not – the topic of privacy and data protection in contrast to European situations.

This paper takes an interdisciplinary approach to the comparative exploration of the limitations of privacy in Latin America, bringing together insights from business, media and communications, and law to offer a holistic analysis. The discussions here adopt a comparative focus, through an assessment of the conflict between privacy and data sharing, and the collection of data for a significant public health response. The discussion then advances to consider the responses to the pandemic through the development of CoronApps in Colombia, Germany, and the United Kingdom, with some, more-limited references to Ecuador**.**[8]

The comparative analysis includes discussions of the accountability in operation in the rapid development and deployment of apps designed to collect sensitive personal information. Finally, the paper draws together the lessons that can be learnt from shared experiences albeit in very different national and legal cultures and offers recommendations for refining the framework of privacy in Latin America – particularly given the 'newness' of data protection across the region. The conclusions offered here highlight the role of privacy, and its different positioning as a national concern in different regions. This paper outlines the need for considerations of tracing systems and data protection laws to avoid a 'one size fits all approach' by positioning privacy as a public good, rather than an opponent of tracing systems.

2. Privacy as a Public Good, Track & Trace Apps, and Covid-19 – A Digital Challenge?

The suggestion that privacy may operate as a public good was raised by Fairfield & Engel,[9] who argue that privacy is not a private good, but rather one that is public. In making such an argument, the suggestion is that if an individual is careless with data, there is a risk of sharing data not just about oneself, but also about others. In order to truly protect privacy therefore, there is a dependency on the others who hold data about that individual – no single person can cherish privacy and be truly protected alone. In their argument, Fairfield and Engel make it clear that in order to hold privacy as a cornerstone of society, everyone must cherish privacy with the same intensity. Where this does not happen, there can only ever be 'suboptimal' levels of privacy achieved. Through the rollout of various track and trace programmes, health services and national governments have seen fit to place privacy at a suboptimal level, notionally in response to the public health crisis presented by Covid-19. This is seen abundantly clearly when leading computer scientists state publicly that privacy ought to be sacrificed in the pursuit of other public goods.[10] Tensions between the public health response to Covid-19, and

[8] References to Ecuador are made as a comparator to Colombia, but accessibility of resources has limited substantive discussions.

[9] Joshua A.T. Fairfield and Christoph Engel, 'Privacy as a Public Good' (2015) 65 *Duke L.J.* 385.

[10] Hannah Boland, 'Sacrifice privacy for public good, says UK's leading computer scientist' (*The Telegraph*, 5 April 2020) <https://www.telegraph.co.uk/technology/2020/04/05/sir-nigel-shadbolt-emergencies-privacy-might-sacrificed-public/> accessed 06 December 2020.

privacy as a public good are almost inevitable competing interests, and yet it is not inconceivable that privacy is a public good which can be protected while data is collated to contribute to the public good of a national response to Covid-19.

Part of the response – across regions – has been to unveil apps to track and trace people who may have been exposed to the virus. These initiatives have – it appears – been dealt with differently across nations. This difference is attributed to the various political systems, but also the cultural differences in every country. For instance, mandatory tracing apps are in use in China, Turkey, and India,[11] while in other states such as Australia, Germany, and the UK, voluntary systems are being utilised. The differences in approach here do not necessarily correlate to distinct differences in neither infection nor mortality rates, but instead reflect a difference in national response traits. Furthermore, it becomes evident that the specific cultural differences have an impact on the pandemic. For example, in terms of cultural dimensions, national cultures are described on a spectrum between individualistic and collectivistic. Latin American countries are often collectivistic and Northern European countries often individualistic.

Moreover, using apps is not a radical step in the smartphone age. The idea of an app to follow, track and trace people who were exposed to a virus is not new. Latonero presented the case for using apps very clearly in 2018, albeit using Ebola as the example that comes into question:

> Consider a response organization asking a mobile phone company for the phone numbers and records of all the users in the country in order to trace the network of individuals who may have become infected. That data would need to be analyzed to locate those at risk, and personal information might be shared with other responders without the consent of the data subjects.
>
> The assumption in such an operational decision is that saving the lives of the person's contacts and protecting the health of the broader public outweigh the privacy concerns over that person's personal information. Yet such decisions about trade-offs, particularly in the case of the Ebola response, remain highly controversial due to the potential privacy violations inherent in collecting the mobile phone records of individuals at a national level without the consent of individuals.[12]

The issues Latonero highlighted in 2018 are now central[13] to debates about the use of the Covid-19 applications developed by governments the world over. The Covid-

[11] Paul Schwartz, 'Illusions of consent and COVID-19 tracking apps' (*iapp*, 19 May 2020) <https://iapp.org/news/a/illusions-of-consent-and-covid-tracking-apps/> accessed 22 July 2020.

[12] Mark Latonero, 'Big Data Analytics and Human Rights' in Molly K Land & Jay D Aronson (eds), *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018) 154-155.

[13] Mark Latonero, 'Big Data Analytics and Human Rights' in Molly K Land & Jay D Aronson (eds), *New Technologies for Human Rights Law and Practice* (Cambridge University Press, 2018) 154-155.

19 aftermath is an excellent working ground for addressing these types of question, since many countries have adopted different approaches regarding the control of movement, privacy and safety of their citizens. The fact that every country (and even states or administrative governments within countries) adopted a different strategy on this front seems to provide evidence on how the supposed objective data relating to the virus leads to different approaches in handling it, based on cultural, social and political structures.[14] Equally, the development of different approaches at different stages of the pandemic is in itself instructive in examining the emerging traits in respect of control versus digital rights.

3. The Rights Conflict: Data Protection v Public Safety?

The unprecedented global pandemic, and associated social lockdowns have caused not just a public health crisis, but also an associated digital rights crisis. Not only are we increasingly dependent on Internet access during such a crisis – for access to news, media content, communications, and work, but also for tracking the spread of the pandemic. This increased dependency has given greater prominence to access to the Internet – which now more than ever needs to be recognised as a fundamental human right[15] – but has also allowed broader discussions relating to data, privacy, trust & transparency, and the hierarchy of rights to emerge into mainstream discourse.

As early as 2 April 2020, over 100 civil society organisations called openly on governments to respect and uphold human rights in the midst of the pandemic, specifically requesting that states do not, “disregard rights such as privacy and freedom of expression in the name of tackling a public health crisis”.[16] This is a particularly powerful and timely reminder of the precarious state of privacy and data protection rights in not only the digital age, but one of unprecedented cross-border crisis. Such civil society concerns serve as a reminder that in some legal jurisdictions, and national territories – such as Germany and the UK – there are greater discussions, considerations, and concerns placed upon the sanctity of personal data and digital rights than in other states. Regardless of those national tendencies – and protections – the Covid-19 crisis has the potential to detrimentally

---

[14] The political influence is not to be understated, especially given the local lockdowns being implemented in England with special powers being handed to local councils, without these councils having access to track & trace data. This is by definition the localising of lockdowns as a political mechanism rather than a legal one.

[15] Merten Reglitz, ‘The Human Right to Free Internet Access’ (2020) *Journal of Applied Philosophy* Vol 3(2) 314.

[16] Open Rights Group, ‘Joint Civil Society Statement: States use of Digital Surveillance Technologies to Fight Pandemic Must Respect Human Rights’ (*Open Rights Group*, 2 April 2020) <https://www.openrightsgroup.org/publications/joint-civil-society-statement-states-use-of-digital-surveillance-technologies-to-fight-pandemic-must-respect-human-rights/> accessed 22 July 2020.

impact upon civil liberties for a prolonged period of time.[17] In turn, whilst international civil society organisations, and even the United Nations work to establish baseline standards for rights protections, it is important to remember that a predominantly Westernised approach is not always suited to Latin American states and systems. It has been mentioned that the Colombian *habeas data* law for the protection of information capture and management "has implied the tropicalization of European norms"[18] leading to important normative gaps and leaving decisions to judicial interpretation. Thus, it was a Westernised adaptation, rather than a local development of Colombian legal system, and a similar thing has taken place elsewhere in Latin America. Despite being a transplanted piece of legislation, it fails to provide safeguards recommended by the OMS such as the rights to opposition, to access and to rectification, exposing the information of citizens under the exceptions of sanitary urgency and emergency, even with little to no regard for previous sentences of the Constitutional Court.[19] The ideal of privacy as a public good,[20] where it serves to protect all, and we should all therefore partake in protecting each other's privacy, is one which is not always the predominant concern in Latin American states. The discourse of protecting all the population is easily manipulated so as to dismiss worries about personal and private information as secondary to national health and safety.

Not all countries have data protection legislation – notable in respect of the lack of approval of the Data Protection Bill in Ecuador[21] – as well as through the concerns voiced in respect of the Colombian privacy law – which has been considered of utmost importance for the protection of the private life of its citizens.[22] Calls by Human Rights Watch have been overlooked, with the Ecuadorean National Assembly continuing to keep the draft bill pending despite the outcry about the data

---

[17] Simon Chandler, 'Coronavirus Could Infect Privacy and Civil Liberties Forever' (*Forbes*, 23 March 2020) <https://www.forbes.com/sites/simonchandler/2020/03/23/coronavirus-could-infect-privacy-and-civil-liberties-forever/> accessed 22 July 2020.

[18] Luis Fernando Cote Peña, 'Hábeas data en Colombia, un trasplante normativo para la protección de la dignidad y su correlación con la NTC/ISO/IEC 27001:2013' (2016) Agencia español de protección de datos <https://www.aepd.es/sites/default/files/2019-10/habeas-data-en-Colombia.pdf>.

[19] Ana Gómez-Córdoba, Sinay Arévalo-Leal, Diana Bernal-Camargo and Daniela Rosero de los Ríos, 'El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia' [The right to personal data protection, digital technologies and the pandemic for COVID-19 in Colombia] (2020) 50 *Rev. Bioética y Derecho* <http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1886-58872020000300017>.

[20] Joshua A.T. Fairfield and Christoph Engel, 'Privacy as a Public Good' (2015) 65 *Duke L.J.* 385.

[21] Human Rights Watch, 'Ecuador: Privacy at Risk with Covid-19 Surveillance' (*Human Rights Watch,* 1 July 2020) <https://www.hrw.org/news/2020/07/01/ecuador-privacy-risk-covid-19-surveillance#> accessed 22 July 2020; Assemblea Nacional, 'Gabriela Rivadaneira will promote the data protection law' (12 July 2016) <https://www.asambleanacional.gob.ec/es/noticia/45016-gabriela-rivadeneira-impulsara-ley-de-proteccion-de> accessed 23 July 2020.

[22] Luis Enriquez Álvarez, 'Paradigmas de la protección de datos personales en Ecuador. Análisis del proyecto de Ley Orgánica de Protección a los Derechos a la Intimidad y Privacidad sobre los Datos Personales' (2017) *Foro Revista de Derecho* (27) 60.

that the government is collecting without any independent oversight body.[23] Significant concerns remain even after Minister of Telecommunications, Andres Michelena, confirmed that the Ecuadorean government had consulted the Court of Constitutional Guarantees to check whether respecting privacy could be avoided in respect of the data the SaludEC app collects.[24] The concerns here persist despite the concerns that linger as to the interrelationship between privacy, and the data to collect – if data can be pseudonymized – as in the German example – then the SaludEC app could enjoy higher uptake, and less criticism.

These contextual issues and the cultural differences highlight the importance of cultural-appropriate implementation strategies, especially as it might be necessary to counter steer against cultural norms like “being social”, as observable in most Latin American countries. Therefore, it is essential to understand the cultural norms in a given country and either adapt to them or go against them – a concept that is described as competitive acceptance in the literature.[25] This is a particularly intriguing state of affairs, especially given the prominence of track and trace programmes, and the commonality of using technology and big data capture to assist in the mapping of, and responses to the pandemic.

Given that the use of apps to track and trace is not confined to a handful of countries, or to selected regions, there is a unique opportunity to examine the responses to the development of these apps, as well as the responses to the concerns raised in respect of the invasiveness of tracing technology. Issues persist though, and increasingly, the use of apps, the collection of data, and the impinging on digital rights and digital freedoms are increasingly being pitched as barriers to tackling the pandemic. This is in part, rhetoric, but also positions digital rights such as privacy as opposed to other priorities such as public health. Moreover, the two are not – and should not be pitched as – mutually exclusive. In the era of big data, and technology, it should be possible to deploy apps to track and trace whilst ensuring that privacy rights are upheld, and accountability is maintained. Physical liberties have already been put in a fragile state through various lockdowns – digital liberties should offer a sense of emergence and should form part of the solution. The use of apps is a cornerstone of the Covid-19 response, but, as de Montjoye states, there is a need for a balance: “Contact tracing requires handling very sensitive data at scale,

---

[23] Human Rights Watch, ‘Ecuador: Privacy at Risk with Covid-19 Surveillance’ (*Human Rights Watch,* 1 July 2020) <https://www.hrw.org/news/2020/07/01/ecuador-privacy-risk-covid-19-surveillance#> accessed 22 July 2020.

[24] Gonzalo Salano, ‘Ecuador uses technology to fight COVID-19’ (*AP,* 16 April 2020) <https://apnews.com/516d5ddc49e3436c8681356a640c6a46> accessed 22 July 2020.

[25] Christian Scholz and Volker Stein, *Interkulturelle Wettbewerbsstrategien* (Vandenhoeck & Ruprecht 2013).

and solid and proven techniques exist to help us do it while protecting our fundamental right to privacy. We cannot afford to not use them."[26]

4. Confronting the Covid-19 Pandemic with Technology: The Rise of the Coronapps

The discussion that follows here considers app development – and concerns – in each of the nations of Colombia, Germany, and the UK. The rollout of the various apps highlights the different developmental stages and concerns in the different countries, but also reflects the management of the pandemic in each of these legal jurisdictions. We turn first to Colombia, and its CoronApp.

4.1. The Colombian CoronApp

It is interesting to note that the Colombian "CoronApp" predates the development and release of the German and UK apps (both of which were developed as lockdown restrictions begun to be lifted), having been released on the 7th of March, 2020,[27] although it was built on top of a 2017 App designed as an information system and monitoring tool for massive gatherings in the wake of Pope Francis I's visit to the country.[28] By 9 March 2020 – within two days of its release – Privacy International was already voicing concern about potential flaws with the App, based on a concept developed by the Karisma Foundation.[29] Despite the shortcomings, the Colombian government went full-throttle in promoting the App, offering 1 GB of free data and 100 air minutes for those who download the App and registered through it.[30] Moreover, the Colombian government entered an agreement with Samsung, one of the best-selling mobile phone companies in the country, through which the CoronApp installed itself once the user had downloaded and installed the latest

[26] Caroline Brogan, 'COVID-19 contact tracing apps: 8 privacy questions governments should ask' (*Imperial College News*, 2 April 2020) <https://www.imperial.ac.uk/news/196656/covid19-contact-tracing-apps-privacy-questions/> accessed 23 July 2020.

[27] Ministry of Health, 'CoronApp – Colombia, the application to know the evolution of the coronavirus in the country' (*Ministry of Health*, 7 March 2020) <https://www.minsalud.gov.co/Paginas/CoronApp.aspx> accessed 22 July 2020.

[28] Semana, '"La utilidad de CoronApp está en duda": coalición de derechos digitales' (*Semana*, 22 May 2020) <https://www.semana.com/tecnologia/articulo/informe-de-coalicion-de-derechos-digitales-no-ve-utilidad-de-coronapp/673581> accessed 22 July 2020.

[29] Privacy International, 'Colombia: Coronapp fails at public information purpose' (*Privacy International,* 9 March 2020) <https://privacyinternational.org/examples/3435/colombia-coronapp-fails-public-information-purpose> accessed 22 July 2020.

[30] El Ministerio de Technologias, 'Con descarga de CoronApp Colombia, usuarios de telefonía móvil prepago obtendrán internet y minutos de voz gratis durante un mes' (*Presidencia,* 24 April 2020) <https://id.presidencia.gov.co/Paginas/prensa/2020/descarga-CoronApp-Colombia-usuarios-telefonia-movil-prepago-obtendran-internet-minutos-voz-gratis-durante-un-mes-200424.aspx> accessed 22 July 2020.

system security update in their Samsung phone without informed consent.[31] The government also asserted – in efforts to build trust – that the App was created by the Agencia Nacional Digital - AND (National Digital Agency) – a public/private entity (rather than the government) whose task is to "dynamize the construction of a more efficient, transparent and participative State".[32] However, in the information on the App itself, under the "Acerca de CoronApp" (About CoronApp) section, there is no mention of the AND, and on the Google Play Store it appears as created by the INS. The information provided about the App on the AND webpage[33] differs from the information you find in the App, bringing into question the transparency of the effort.

The Karisma Foundation, an NGO dedicated to studying cases of privacy-breach in Colombia, has done a series of reports on the App. Lately it dismissed the App altogether, saying it does not work and it will not work, because of the lack of transparency regarding the handling of the data, the apparent trial-run done by the AND on the tracing feature, and the fact that it is using a centralized rather than a decentralized database.[34] In the congressional debate held on the 16th of June, senator Juanita Goebertus received contradictory replies from different levels of government and the INS regarding the data that will be stored, how, and for how long. She finally stated that the lack of a clear policy regarding the handling of the information could be responsible for the very limited usage of the App, spreading to less than 12% of the population.[35] The concerns raised here, are similar to those raised by the AND eventually, when it came out in criticism of the App, suggesting that the cultural mistrust of the government when it comes to data, is more widespread than is reported. In essence, this tension does not play out through privacy as a public good, but rather because of the cultural tendencies to comply with authoritarian regimes. Trends have emerged – through NGOs such as AND, as well as through senatorial questions, as to the situation with data and privacy. While slow to emerge, these represent widespread elements of mistrust in the natural traits in Colombia.

In order to explore further the risk to privacy, the conflict of rights, and approaches to data protection, we look at the approaches taken elsewhere to compare it with the Colombian CoronApp. The approach adopted in Germany is considered first.

---

[31] Las2orillas, 'La jugadita de Samsung y el gobierno con la aplicación CoronApp' (*Las Orillas*, 23 May 2020) <https://www.las2orillas.co/la-jugadita-de-samsung-y-el-gobierno-con-la-aplicacion-coronapp/> accessed 22 July 2020.

[32] Agencia Nacional Digital <https://and.gov.co/> accessed 22 July 2020.

[33] Agencia Nacional Digital, 'LA HISTORIA DETRÁS DE CORONAPP' (*Agencia Nacional Digital,* 4 May 2020) <https://and.gov.co/news/la-historia-detras-de-coronapp/> accessed 22 July 2020.

[34] Carolina Botero, 'CoronApp neither works nor will work' (Fundación Karisma, 28 June 2020) <https://web.karisma.org.co/coronapp-ni-funciona-ni-funcionara/> accessed 22 July 2020.

[35] AlianzaVerde, 'Debate a CoronApp sin respuestas": Representante Juanita Goebertus.' (*Alianza Verde,* 16 June 2020) <https://www.alianzaverde.org.co/liderando-congreso/debate-a-coronapp-sin-respuestas-representante-juanita-goebertus> accessed 22 July 2020.

4.2. Corona-Warn-App in Germany

In Germany, the so-called "Corona-Warn-App" was released on the 16th of June 2020 and was published by the Robert Koch-Institut. The app was developed by SAP and the Deutsche Telekom. From a technological perspective, the app utilized the interface protocol designed by Apple and Google. With nearly 16 million downloads on the 13th of July, the app can be considered a success because of its uptake numbers in such a short space of time.[36] Although the open-source and decentralized approach is highly praised,[37] the German government preferred a centralized and more intrusive procedure. It is therefore evident that the technological change was based on the public discourse through NGOs and developers that forced the government to rethink their approach.

In Germany, data privacy is a valued good, and there is still a vivid community that fights for net neutrality.[38] The Chaos Computer Club (CCC) is the most prominent organization that fights for privacy and data protection. Consequently, they issued an open letter concerning the proposed centralized approach for the Corona App.[39] In that letter, they predicted the failure of an App, which is optional to use, that cannot create any trust in the user. Furthermore, they highlight that there is a risk of misuse. In short, movement data is sensitive and requires protection, but data about the potential infection may be even more harmful. The CCC states that complete surveillance of movement data and the access to health data may be a horror-scenario. If it were possible to de-anonymize, the *gläserne Bürger* (glass citizen) would be possible.

As a result, it becomes apparent that the proposed approach by the government would lead to dangers for society, especially as the app mimics a black box. Interestingly the main stakeholders in the smartphone market, Apple and Google, also prefer a decentralized approach.[40] This strategy is surprising, as both companies can be seen as *Datenkrake* (data hydras), and have data-driven commercial business models. IT-experts from CCC and many other NGOs, as well as Apple and Google, focused on a decentralized approach. Given that it is deemed

---

[36] Robert Koch Institut, 'Disrupt infection chains digitally with the Corona warning app' (*Robert Koch Institut*, 17 July 2020) <https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/WarnApp/Warn_App.html> accessed 22 July 2020.

[37] Dominik Rpzeka, '"Run exemplary" Chaos Computer Club praises German Corona app' (zdfheute, 16 June 2020) < https://www.zdf.de/nachrichten/politik/corona-app-launch-100.html> accessed 22 July 2020).

[38] Tobias M Scholz, ‚Die Konvergenz der Digitalisierung – eine Prognose für Europa' in: Christian Scholz, Peter Dörenbächer, and Anne Rennig (eds.) *Europa jenseits des Konvergenzparadigmas Divergenz – Dynamik – Diskurs, Nomos* (Baden-Baden) 2019, 357-375.

[39] Chaos Computer Club, 'Corona tracing app: Open letter to the Federal Chancellery and Minister of Health' (*Chaos Computer Club,* 24 April 2020) < https://www.ccc.de/de/updates/2020/corona-tracing-app-offener-brief-an-bundeskanzleramt-und-gesundheitsminister> accessed 22 July 2020.

[40] Apple, 'Privacy-Preserving Contact Tracing'<https://www.apple.com/covid19/contacttracing> accessed 22 July 2020.

essential, the app needs to be widely used in the general population to be effective, and if it is spread in popularity efficiently, it becomes a dangerous tool ripe for misuse. People need to trust the app utilization as well as the people behind the app. Therefore, CCC described contact tracing as a high-risk technology and produced ten criteria on which contact tracing apps need to be evaluated:[41]

1. *Epistemological use & appropriation to the purpose:* It is essential to prove that any contact tracing app will help to fight against Covid-19 and that any data is solely used for this fight
2. *Voluntary and non-discriminatory:* Any app that needs to used freely and people who are not using the app should not fear any disadvantages by that.
3. *Fundamental privacy:* Anonymization and cryptography are the core of any app and need to ensure the safety and privacy of the users. There need to be the highest standards for privacy, and they need to be enforced by the legal entities
4. *Transparency and verifiability:* The whole source code needs to be open-source, and it should be possible to test and verify the app individually and freely
5. *No central entity that we must trust:* A central server is not a must-requirement for contact tracing from a technological point of view. Therefore, it is not necessary to build upon the central approach
6. *Datensparsamkeit (data minimization):* It is essential to collect only the data that is necessary for contact tracing. Even if data is gathered for epidemiological research, the user needs to accept this utilization.
7. *Anonymity:* Any data collected by the app needs to be anonymized, and, most fundamentally, nobody can de-anonymize the data.
8. *No installation of central movement and contact profiles:* The app needs to be programmed that is impossible to create profiles of movement and contacts even if it may be unintended. Logging through GPS, phone number, or social media should be refused.
9. *Unchainable:* It is essential that any ID needs to be protected, and the underlying chain of contact is never derivable from other data. Only with the right key, the contact chain can be revealed
10. *Unobservability of communication:* Even if communication in the system is observable, it is crucial that nobody can find out that a person may be infected or was in contact with an infected person.

It is still unclear if the social influence or the power of Apple and Google led to the change in strategy. However, due to the approach of open source code and a relative data minimizing approach, it seems that the government listened to CCC and other NGOs. Even though the CCC is still suspicious of the government, they are no

[41] Chaos Computer Club, ’10 touchstones for the assessment of “Contact Tracing” apps’ (*Chaos Computer Club*, 6 April 2020) < https://www.ccc.de/de/updates/2020/contact-tracing-requirements> accessed 22 July 2020.

longer criticizing the app.[42] It is somewhat surprising for everybody that a government-initiated app may follow the criteria mentioned above but such surprise led to CCC-spokesperson, Linus Neumann, stating that CCC found no noteworthy shortcomings and added that this situation is confusing for him as well![43] The – if not quite praise – then wide acclaim for the approach of the app from the CCC focused around the decentralized and pseudonymized data storage, and general all-round privacy friendly development. While there is little evidence as to *why* the Government followed the CCC recommendations, it is reasonable to conclude that the influence of the CCC – and its support – would be critical in ensuring widespread downloading of the app as a cornerstone of the Covid-19 response in Germany.

The NGO Netzpolitik.org also discussed the app and highlighted that its development was promising.[44] It seems that societal debate led to significant changes, and ultimately, a lot was "done right." The code is open source, while the community has a chance to discuss obstacles in the code and propose changes. The decentralized approach helps issues with anonymity and usage given the scepticism of society. The app was designed to minimize data collection and yet a study by YouGov at the release date shows that the country may be split into two camps, with only half the population intending to use the app.[45] Moreover, the app may not work with some smartphones, leading to technological discrimination as well as the digital divide concerning age and economic status.[46]

Even though the app seemed quite successful after nearly a month's usage, it still needs more users. The Corona-Warn-App can be seen as a successful tool based on its technical merits. The app is decentralized and open source; it focuses on many criteria the CCC derived. And still, there is a high degree of scepticism. Furthermore, the path to digitized society is not yet finished. People are not all connected to a smartphone, and not every smartphone is capable of using this app. There is an underlying bias within any contact tracing app, that even one of the seemingly best apps currently existing, cannot overcome.

The Corona-Warn-App has seen some – albeit limited – success, and sets out a benchmark for other European schemes to aspire to, and has arguably influenced

---

[42] Susanne Höb, ‘Corona app: Chaos Computer Club makes no recommendation’ (*Berliner Morgenpost,* 30 June 2020) <https://www.morgenpost.de/politik/article229394400/Corona-App-Daten-Sicherheit-Chaos-Computer-Club-Kritik.html> accessed 22 July 2020.

[43] T3N, ‘The government is trolling the CCC with this “nasty trick”’ (*T3N,* 22 June 2020) <https://t3n.de/news/corona-warn-app-ccc-1293138/> accessed 22 July 2020.

[44] Markus Beckedahl, ‘Much has been done correctly’ (*Netzpolitik.org,* 15 June 2020) <https://netzpolitik.org/2020/vieles-doch-noch-richtig-gemacht/> accessed 22 July 2020.

[45] YouGov, ‘Pressegrafiken: Corona-Warn-App 17-19 June 2020’ (*YouGov,* 22 June 2020) <http://www.yougov.de/pressecharts_Corona_Warn_App> accessed 22 July 2020.

[46] Federal Institute for Risk Assessment, ‘A quarter say they use the Corona warning app’ (*BfR,* 26 June 2020) <https://www.bfr.bund.de/de/presseinformation/2020/23/ein_viertel_gibt_an__die_corona_warn_app_zu_nutzen-248780.html> accessed 22 July 2020.

other nations in making their own apps open-source.[47] Going open-source and having an open discussion about the development helped the app to gain trust and achieve some form of transparency. There is no backdoor or other malware in the app, so, even if there is mistrust in the developing companies or the government, if NGOs like the CCC are supporting the app, this creates widespread trust. The NHSX app in the UK has adopted a different approach, and it is to an examination of that track & trace scheme that we turn to next.

4.3. NHSX Track & Trace in the UK

The management of Covid-19 through so-called 'track and trace' systems across the different territories within the UK has caused little short of national ridicule, but beyond that, evidences the dangers of untested and untried pieces of technology that rely on population trust. The farce that the NHSX Track & Trace programme descended into begets the divergence of approaches that have played out across England & Wales; Scotland, and Northern Ireland – who have all developed alternate app systems as part of the devolved management of the Covid-19 pandemic.[48] The 'joined up' approach has fallen flat, with Scotland, and Northern Ireland preferring apps that meet their specific requirements within each respective legal territory, rather than being thrown together as part of the UK-wide approach mandated by Westminster. Concerns have dogged the NHSX track & trace app since its ill-conceived introduction. The UK Government first piloted its contact-tracing app – a dedicated app developed by the National Health Service (NHS) in its Covid-19 app – in May 2020 and launched it on the Isle of Wight as a trial on 28 May 2020. The NHSX Covid-19 app was hailed as the forefront of the UK Government battle against Covid-19 despite *not* following the architecture of the Google and Apple app.

In the UK, the approach adopted by Her Majesty's Government has been one of fiasco,[49] misstep, and blasé assumptions about the willingness of the populace to follow the Government requests to download and share – openly – data with the Government itself. The short-lived NHSX Covid-19 app was swiftly abandoned on 18 June,[50] despite Prime Minister Johnson's assertions in late May that there would be

[47] Andrea Downey, 'Code for Ireland's Covid Tracker app given to global public health project' (*Digital Health Net*, 23 July 2020) <https://www.digitalhealth.net/2020/07/code-for-irelands-covid-tracker-app-given-to-global-public-health-project/> accessed 23 July 2020.

[48] Angela Daly and Maurice Mulvenna, 'UK contact tracing apps: the view from Northern Ireland and Scotland' Ada Lovelace Institute (24 September 2020) <https://www.adalovelaceinstitute.org/blog/uk-contact-tracing-apps-the-view-from-northern-ireland-and-scotland/> accessed 06 December 2020; Matt Reynolds, 'The UKs contact tracing plan has two fatal flaws' (*WIRED News*, 22 May 2020) <https://www.wired.co.uk/article/uk-coronavirus-contact-tracing-testing-flaws> accessed 06 December 2020.

[49] Oliver Wright and Tom Knowles, 'Coronavirus app failure leaves tracing plan in disarray' (*The Times*, 19 June 2020) < https://www.thetimes.co.uk/edition/news/huge-u-turn-as-virus-tracking-app-is-axed-rf3nh66kq> accessed 22 July 2020.

[50] Laura Donnelly and Mike Wright, 'NHS coronavirus contract-tracing app ditched in major U-turn' (*The Telegraph*, 18 June 2020) <https://www.telegraph.co.uk/news/2020/06/18/nhs-coronavirus-contact-tracing-app-ditched-major-u-turn/> accessed 22 July 2020.

a 'world-beating'[51] system in operation in Britain to lead the way in lifting lockdown restrictions. The abandonment of the home-grown app was not just one brought about by the lack of trust in the Government, but also in the app itself. The move to the Apple / Google variant of the app was made for – at least notionally – technical tracing reasons once it became apparent that the NHSX Covid-19 app was not fit for purpose and was only detecting 1 in 25 contacts on Apple iPhones.[52] In reality, there are a number of significant hurdles that the NHSX Covid-19 app had to overcome – and in which it was found to be lacking.

Significantly – and perhaps most prominently – when the app trial was rolled out across the Isle of Wight with a population of 140 000, between 50 000 and 60 000 people downloaded it.[53] A confirmed figure of downloads is tricky to pinpoint, especially given concerns that the number of downloads may actually be lower, as some people may have downloaded the app more than once, or it may have been downloaded by those not actually on the Isle of Wight.[54] These flaws – whilst significant given the reliance on data collection, and indeed, data sharing – raise serious questions about the security and integrity of the app itself. More pressing concerns about the data sharing expected – and the security of that personal data – were raised before the trial was concluded. The most serious issues relate to the information that the app collates – which, given its operation based on Bluetooth, and requires on Android phones location services to be enabled, are significant, and despite scrutiny taking place in the Houses of Parliament, the app trial was described as 'enormously successful' with 'huge'[55] take-up rates – a matter of some debate given the issues with the figures, and the subsequent abandonment of app and trial. Volpicelli argues that the real reason for the trial of the NHS Covid-19 app was to get the public used to the idea of being traceable and being tracked, rather than for the app to have a significant impact upon the infection rates.[56] This is in part,

---

[51] Reuters, 'UK PM Johnson vows "world beating" track and trace COVID system by June 1' (*Reuters*, 20 May 2020) <https://www.reuters.com/article/us-health-coronavirus-britain-track-idUSKBN22W1MW> accessed 22 July 2020.

[52] Laura Donnelly and Mike Wright, 'NHS coronavirus contract-tracing app ditched in major U-turn' (*The Telegraph*, 18 June 2020) <https://www.telegraph.co.uk/news/2020/06/18/nhs-coronavirus-contact-tracing-app-ditched-major-u-turn/> accessed 22 July 2020.

[53] There are discrepancies in reporting, with some reports suggesting the figures reached 60 000+ according to Gian Volpicelli, 'What's really happening with the NHS Covid-19 app trial' (*Wired,* 16 June 2020) <https://www.wired.co.uk/article/contact-tracing-app-isle-of-wight-trial> accessed 22 July 2020, whereas other reports more conservatively put the number at 50 000 (Matt Burgess, 'Everything you need to know about the NHS test, track and trace app' (*Wired,* 18 June 2020) <https://www.wired.co.uk/article/nhs-covid-19-tracking-app-contact-tracing> accessed 22 July 2020).

[54] Tom Morgan, 'Isle of Wight contact tracing trial undermined by people on UK mainland downloading the app' (*The Telegraph*, 23 May 2020) <https://www.telegraph.co.uk/news/0/isle-wight-contact-tracing-trial-undermined-people-uk-mainland/> accessed 22 July 2020.

[55] HL Deb 19 May 2020, vol 803, col 1089.

[56] Gian Volpicelli, 'What's really happening with the NHS Covid-19 app trial' (*Wired,* 16 June 2020) <https://www.wired.co.uk/article/contact-tracing-app-isle-of-wight-trial> accessed 22 July 2020.

understandable because of the notion that one must download an app and carry one's phone everywhere – which could in part be more intrusive than anticipated.

At the behest of the Government, a 'voluntary' app was being rolled out that actively tracks locations and identifies who else you have been in proximity to. What is particularly interesting is that not only did the NHSX Covid-19 app get abandoned on – notionally – grounds of technical limitations, but the shift to endorse and use smartphone functionality from the 'app' experts of Apple & Google,[57] indicates a fundamental misunderstanding of the values of the public. For instance, the Isle of Wight trial highlighted – at best – a less than 50% take-up rate of a Government backed and developed app. That was, perhaps not the smartest move designed to build trust, especially given that Google – producer of Android software – and Apple – producer of iPhones and the iOS software are two of the largest technology producers, and two of the three entities with the largest presence in the smartphone market in the UK. To put it differently, the public already trust Apple and Google with their personal data – some of it much more intrusive, such as the Health apps on iPhones – much more than the NHSX Covid-19 app.

The intrusiveness of the app, and of the need to carry a phone everywhere remains a problem of the 'always on' generation, and digital dependency, despite the increasing push for privacy as a public good to be a working norm in Europe. It also rests on the presumption that everyone has – and can afford – a compatible smartphone, which is a sweeping assumption about technological affordability,[58] and the digital divide at times of unprecedented financial and economic hardship.[59] The use of the Google / Apple ecosystem in part addresses the intrusiveness concerns, not least because of the public willingness to trust these two commercial actors with their data – much more readily, even pre-pandemic. Yet because trust, and transparency was not apparent in the Government app, public willingness was not as abundant in using a Government app. Ultimately on 18 June, the UK Government switched to the decentralised Apple-Google model for its virus tracing software.[60] This is unsurprising given the concerns that privacy campaigners and groups have expressed in light of the track and trace apps.

---

[57] Zoe Kleinman, 'Coronavirus: New Covid-19 tracing tool appears on smartphones' (*BBC News*, 20 June 2020) <https://www.bbc.co.uk/news/health-53120290> accessed 22 July 2020.

[58] Sonia Jorge, '2019 Affordability Report' (*Alliance for Affordable Internet*, 2019) <https://a4ai.org/affordability-report/report/2019/> accessed 23 July 2020.

[59] Mercedes Garcia-Escribano, 'Low Internet Access Driving Inequality' (*International Monetary Fund*, 29 June 2020) < https://blogs.imf.org/2020/06/29/low-internet-access-driving-inequality/> accessed 23 July 2020; Pedro Nicolai da Costa, 'Digital Divide Becomes 'Chasm' as Covid-19 Drags On' (*Forbes*, 30 June 2020) <https://www.forbes.com/sites/pedrodacosta/2020/06/30/digital-divide-becomes-chasm-as-covid-19-pandemic-drags-on/#66ce82947fba> accessed 22 July 2020.

[60] Leo Kallon, 'UK virus-tracing app switches to Apple-Google model' (BBC News, 18 June 2020) <https://www.bbc.co.uk/news/technology-53095336> accessed 22 July 2020; Mariano Delli Santi, 'NHSX App Delayed, but Data Protection Still MIA' (*ORG Blog*, 23 June 2020) <https://www.openrightsgroup.org/blog/nhsx-app-has-been-delayed-but-data-protection-is-as-urgent-as-ever/> accessed 22 July 2020.

Concerns have been raised throughout the pandemic about the UK app by the leading privacy and digital rights advocacy group in the UK, the Open Rights Group (ORG). In April 2020, ORG highlighted that there was a need to explain:

1. What safeguards and scrutiny will be provided to safely allow for the "tracking" of individuals.
2. What other data, combined with traffic or location data, may be necessary to effectively combat the spread of coronavirus.
3. What conversations it has had with other governments on cross-border data initiatives to prevent the spread of coronavirus.
4. How the Government are engaging with PEPP-TP.
5. The Government's criteria for assessing the different technology approaches to contact tracing apps.
6. If the Government is to adopt technology solutions for monitoring the spread of the virus after lifting the lock-down, and whether it will commit to the strongest strong privacy-preserving model to combat the spread of the virus.[61]

The concerns of ORG were significant enough that the NHS Test and Trace scheme in the UK was threatened with court action unless the Government undertook an assessment of data protection implications.[62] Such a step was taken by ORG in light of the fact that there was seemingly no data protection impact assessment (DPIA)[63] conducted, but also because the privacy notice in the Test and Trace scheme fails to differentiate between personal data, and special category data.[64] Similarly, the notice relies upon the Americanisation of 'personally identifiable data'[65] instead – not something enshrined in law in the UK. Perhaps the most significant concern alongside these is that the app itself suggested that data would be retained for a period of 20 years.[66] Such a position indicates that the Government is ignoring legal

---

[61] Open Rights Group, 'Covid-19 and Personal Data: April Briefing' (*ORG*, 7 April 2020) <https://www.openrightsgroup.org/publications/covid-19-and-personal-data-april-briefing/> accessed 22 July 2020.

[62] Open Rights Group, 'Government Admits Test and Trace Unlawful' (*Open Rights Group,* 20 July 2020) <https://www.openrightsgroup.org/press-releases/government-admits-test-and-trace-unlawful/> accessed 22 July 2020; Laurie Clarke, 'Digital rights group report NHS Test and Trace to ICO, claims legal breach' (*New Statesman*, 4 June 2020) <https://tech.newstatesman.com/gdpr/open-rights-group-reports-nhs-test-and-trace-to-ico> accessed 22 July 2020.

[63] Required under s64 Data Protection Act 2018 which states that wherever there is a type of data processing "which is likely to result in a high risk to the rights and freedoms of individuals" a data protection impact assessment is required.

[64] Which includes data revealing racial or ethnic origins; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; health; sex life; sexual orientation. See Data Protection Act 2018, Schedule 1.

[65] As listed in the Data Protection Act 2018, Schedule 1.

[66] NHS Test and Trace Privacy Information: <https://contact-tracing.phe.gov.uk/help/privacy-notice> accessed 22 July 2020.

obligations in respect of data protection, but also eschewing calls for protections[67] to be embedded in new privacy legislation too. The latter suggestion was resoundingly shouted down by the Secretary of State for Health, and brushed aside as though minor – a point noted with disappointment by the Human Rights Committee on 7 May 2020[68] despite suggestions being made in respect of this requirement.[69] Ultimately, the Secretary of State for Health had to admit the lack of DPIA and the consequent unlawfulness of the Covid-19 tracing programme in July 2020,[70] reflecting the importance of the work of the ORG in protecting privacy rights.

All of these concerns are significant, highlighting the very real risks that the so-called anonymity[71] of the programme to test and trace is at best a minor inconvenience and was never at the heart of the plan – perhaps initially for understandable reasons. The dangers though – despite the political wrangling and high-level complaints lodged with the Government – are much more 'real' on the ground. Notably, in light of the lack of thought given to privacy and safety, reports are emerging of abuses of the system by those required to play a role within it. For instance, reports are emerging of people being contacted through social media platforms by staff from pubs and restaurants. These reports allege that people are being contacted – for amongst other things, dating – based on their details being left at pubs or restaurants as part of the track and trace programmes.[72] Not only does this cast doubt upon who can act as a contact tracer, but also highlights the vulnerabilities of the system which is predicated on trust at all levels, and which is open to abuse. It also prejudices the potential uptake of a track & trace app, if it is open to abuse by complying with government regulations implemented to contain the pandemic – such as leaving contact details with commercial venues.

---

[67] Laurie Clarke, 'Government says no to new privacy legislation for NHSX contact tracing app' (*New Statesman,* 22 May 2020) <https://tech.newstatesman.com/gdpr/government-privacy-legislation-nhsx-app> accessed 22 July 2020.

[68] Harriet Harman (22 May 2020) <https://twitter.com/HarrietHarman/status/1263755692655157249?s=20> accessed 22 July 2020; Matt Hancock, 'COVID-19 Safeguards Bill Letter' (21 May 2020) <https://committees.parliament.uk/publications/1223/documents/10345/default/> accessed 22 July 2020.

[69] Lilian Edwards and others, 'The Coronavirus (safeguards) Bill 2020: Proposed Protections for Digital Interventions and in Relation to Immunity Certificates' (13 April 2020) <osf.io/preprints/lawarxiv/yc6xu> accessed 22 July 2020.

[70] RT.Com, '"Reckless": Privacy rights group lashes out at UK govt after it admits Covid-19 Test and Trace program didn't follow legal rules' (*RT.com*, 20 July 2020) <https://www.rt.com/uk/495261-privacy-covid19-test-trace-unlawful/> accessed 22 July 2020.

[71] Laurie Clarke, 'NHS test and trace privacy doc throws doubt on app's "anonymity" claims' (New Statesman, 28 May 2020) <https://tech.newstatesman.com/coronavirus/nhs-test-and-trace-privacy-doc-throws-doubt-on-apps-anonymity-claims> accessed 22 July 2020.

[72] Tali Fraser, 'Has the abuse of 'test and trace' started already?' (The Spectator, 12 July 2020) <https://www.spectator.co.uk/article/has-the-abuse-of-test-and-trace-started-already-> accessed 06 December 2020. Other similar reports of 'abuses' of the tracing programmes have also arisen: FR24 News, 'Woman says bartender used coronavirus tracking information to send Facebook message' (11 July 2020) <https://www.fr24news.com/a/2020/07/woman-says-bartender-used-coronavirus-tracking-information-to-send-facebook-message.html> accessed 06 December 2020.

In light of all of these deficiencies with the UK system, Her Majesty's Government are keen to adopt incentives in a revamped NHS tracing app to try and "win over a sceptical public and revitalise the troubled project".[73] The proposed changes suggest that personal benefits such as those triggering notifications through wearable technology will be introduced. These suggestions – whilst potentially beneficial – are likely to ensure yet more privacy concerns emerge – not least from Apple, who have raised questions about the precise location function proposed to be used in developing these changes.[74] Not only this, but the very notion that the Government can tap into 'Fitbit' style solutions at the very time the European Commission is determining whether Google and Fitbit be allowed to merge[75] suggests a further misreading of the public mood relating to data sharing, whilst raising further issues about the sensitivity of the information collected.[76]

What all of these examples – from Colombia, Germany, and the UK indicate, is that there is a shared approach to the implementation of a tracing app. In the enduring Covid-19 public health crisis, despite differences of approach to privacy, many countries including Colombia, Germany, and the UK are *all* turning to technology to gather data and inform the response. What is also an emerging trend, is the absence of shared practice and expertise in developing an app which values tracing to tackle the pandemic whilst also prioritising data protection – the two should not be mutually exclusive and yet this is how they are positioned by the states requiring their development. Intriguingly, the divergent approaches offer some scope for Latin America to enhance their apps and develop their data protection provisions simultaneously – it is to this that the discussion now turns.

5. Reflections from Europe – Recommendations for Latin America

Based on this analysis, it becomes evident, that even though the virus is borderless and has no "culture", cultural differences have a hefty influence on the design of a Corona App as well as the implementation strategy of such an App. Any tracing app requires a certain amount of diffusion in the public to even work properly, consequently there is a digital version of herd immunity, when it comes to tracking the virus. There are many approaches for how to deal with the cultural differences across the respective countries. The differences between Germany and UK reveal that there are diametral paths to tackle that. Understanding the reasons for the differences are helpful to deal with the own implementation strategies. Germany has

[73] Rowland Manthorpe, 'Coronavirus: New NHS England contact-tracing app may bring 'personal benefits' (*Sky News*, 22 July 2020) < https://news.sky.com/story/coronavirus-new-nhs-england-contact-tracing-app-will-use-fitbit-style-contact-counts-12033994> accessed 23 July 2020.

[74] Op. cit.

[75] Foo Yun Chee, 'Google offers data pledge in bid to win EU okay for Fitbit buy' (*Reuters,* 13 July 2020) <https://uk.reuters.com/article/us-fitbit-m-a-alphabet-eu-exclusive/exclusive-google-offers-data-pledge-in-bid-to-win-eu-okay-for-fitbit-buy-idUKKCN24E2X5> accessed 23 July 2020.

[76] Cory Doctorow, 'Your Objections to the Google-Fitbit Merger' (*EFF*, 25 June 2020) <https://www.eff.org/deeplinks/2020/06/your-objections-google-fitbit-merger> accessed 23 July 2020.

a long history of data protection,[77] as well as a strong focus on trust and transparency. Therefore, it might seem excessive for other countries and probably for many Latin American countries. However, these measurements could be effective in Latin American countries with a high mistrust in the Government. Especially the utilization of open-source might be a way for establishing transparency and by that trust in the app, if there is a lack of trust in the government. The examples in the UK and Germany show that it is not sufficient to just highlight that such an app is useful to flatten the curve, there are many issues entangled on a more emotional and cultural level. Consequently, the cultural aspects of the public are one of the core issues that the implementation strategy needs to focus on, especially as from a technological point of view, creating this app is straight-forward. But how transparent or untrustworthy such an app is, is a decision significantly influenced – and shaped – by the government.

It is therefore evident – and understandable – just how legislation on privacy protection comes as secondary concern in Latin America in contrast to those issues that are considered to be of collective interest. The cultural tendencies towards respecting authoritarianism and acquiescing to such higher powers manifests itself through pushing data protection and privacy concerns aside so as to allow other issues to dominate. Similarly, legislation implies compliance, something that is clearly problematic in Latin America, given the cultural and social norms, and the governance structures. It is, on balance, a markedly different system to that in Germany and the UK, and a ‘one-size fits all approach’ will be of very limited success.

Two everyday expressions seem to explain a lot of what happens in the chasm between legislation and action. The first one is *se obedece, pero no se cumple* [it is obeyed, but not executed], a seeming tradition of the Spanish colonies during the colonial times to visibly show deference to the laws enacted by the monarchy, while at once avoiding their enforcement because of practical or idiosyncratic reasons.[78] This impossibility of enforcement has been pointed out as typical of developing countries.[79] The second expression is *hecha la ley, hecha la trampa*, roughly translated by Miller[80] as “when you pass a law, you create a loophole”, meaning that as soon as a law is enacted, a way around it is also developed. The two expressions amount to a superficial commitment to a law that does not translate into the necessary actions and, then, a clear omission of its requirements based on given loopholes.

---

[77] The German state of Hesse enacted the first Data Protection Act in 1970 (Datenschutzgesetz [Data Protection Act], October 7, 1970) with many other states following quickly. See: Kerstin Tscherpe in *KOMMENTAR ZUM BDSG* 1103 (Jürgen Taeger & Detlev Gabel, eds) 2010.

[78] Clara Ines Guerrero García, ‘Memorias palenqueras de la libertad’ in Claudia Mosquera Rosero-Labbé and Luiz Claudio Barcelos (eds), *Afro-reparaciones: Memorias de la Esclavitud y Justicia Reparativa para negros, afrocolombianos y raizales* (Universidad Nacional de Colombia, 2007) 371.

[79] Lilliana Lizarazo-Rodríguez, ‘Constitutional adjudication in Colombia: Avant-garde or Case-law transplant? A literary review’ *Estudios Socio-Jurídicos* (2011) 13(1), 145, 173.

[80] Toby Miller, *The Persistence of Violence,* (Rutgers University Press) 2020, 3.

The use of tracing apps as a response to the pandemic is not isolated to individual states nor to selected regional groupings, but is seen across Europe, as well as Latin America, and yet the successes – and concerns – are distinct in these two regions. Where there are emerging areas of shared practice, such as the use of tracing apps, the concerns that are raised – whilst similar – are not always as dominant in the media coverage and analysis offered. In particular, while concerns in Germany and the UK are about data protection laws, and compliance, the concerns in Colombia and Ecuador rested on 'selling' the idea of an app to the public, and enticing the public to comply with incentives, rather than addressing privacy concerns initially. What is particularly interesting – and as the research in this paper has shown – is that despite the common goal of the tracing apps in Germany, the UK, and Colombia being to contribute to the management of the pandemic outbreaks, concerns have been raised about all of the tracing programmes. Moreover, the consistent and shared practice of developing an app is seen as a cornerstone of the approach in each of these examples, reflecting a greater trend towards data in public health more generally.[81]

Even in light of the 'Google got rich from your data'[82] concerns – which resulted in a £3.81 billion fine in Europe for breaching anti-trust rules in 2018,[83] there is still greater willingness to trust commercial exploiters of data than there is to trust the Government – this is the case irrespective of legal jurisdiction. Given this willingness, distrust of Governments in some countries is easy to see, particularly through the lens of tracing apps – and yet what is stark, is that society seems much more willing to share its personal data with those that will commercially exploit it instead of those who may use it for more nefarious, oversight, uses. The hangover of Orwellian warnings[84] seems to remain strong in Europe, yet these concerns are not as prominent in Colombia, Ecuador, and Chile,[85] nor Latin America more broadly. In Europe, the concerns and outcry about the invasiveness, the lack of privacy, and the resulting lack of trust was vociferous – and shared across jurisdictions. The concerns meanwhile in Latin America have been less vocal, yet still very much a factor in

[81] For more on health data see for example: Lizzie Presser, Maja Hruskova, Helen Rowbottom and Jess Kancir, 'Care.data and access to UK health records: patient privacy and public trust' *Technology Science* (2015) <https://techscience.org/a/2015081103/>; Elizabeth Parkin and Philip Loft, 'Patient health records: access, sharing and confidentiality' House of Commons Library (No 07103) (15 May 2020) <https://researchbriefings.files.parliament.uk/documents/SN07103/SN07103.pdf>.

[82] Matt Burgess, 'Google got rich from your data, DuckDuckGo is fighting back' (*Wired*, 8 June 2020) <https://www.wired.co.uk/article/duckduckgo-android-choice-screen-search> accessed 22 July 2020.

[83] European Commission, 'Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine' 18 July 2018 <https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581> (accessed 22 July 2020) per Margrethe Vestager.

[84] BBC News, 'Giant database plan 'Orwellian' (*BBC News*, 15 October 2008) <http://news.bbc.co.uk/1/hi/uk_politics/7671046.stm?butt=love> accessed 22 July 2020.

[85] International Law Firm Alliance, 'The legal implications of Contact Tracing in Chile' (*Abdala & CIA Abogados,* 29 May 2020) <https://diazreus.com/wp-content/uploads/2020/06/LATAM_contact-tracing.pdf> accessed 22 July 2020.

discussions surrounding the pandemic response. Above all else, the sharing of data in Europe seems to concern people minimally when it comes to commercial parties like Google and Apple, yet the same sharing with governments is met with fear, and outcry – very different to the situation in Latin America, which serves to highlight the divergent approaches, but also the compliance tendency with government mandates, even where there are significant fundamental freedoms risks.

Following the European model *could* have benefits for tracing apps in other regions – yet these are unlikely to be workable given the deficiencies in the data protection laws. The norms of privacy as a public good are very much Westernised in their focus – they work where there is collective 'buy in' to the overall picture, and are less suited to situations and cultures, where there is an authoritarian overtone. Privacy can only be utilised in the public interest, if there is a critical mass supporting this perspective – until such a position is reached, concerns such as those seen in Latin America over tracing apps will continue to be raised, but will continue to be brushed aside. Privacy as a public good is a normalised ideal – it is not suited to each system.

6. Conclusion

The vastly different structures, constitutional arrangements and systems of managing personal data collections do not necessarily mean that the same values are prioritised in each nation. In Europe, the situation is more mixed, whereas in Latin America, the results have been stated to be much less impactful.[86] In all countries and in both regions considered here, concerns have been raised about tracing apps, privacy, data protection, and accountability for such systems. Across Europe, the demand for respect for privacy and data protection has been a dominant force in the ways in which tracing apps have been refined. While similar concerns have arisen in Latin America, they have played out as more insignificant – privacy has been pushed aside in deference to public health. Cultural tendencies in Europe to protect individual information have not played out in the same ways in Latin America – mistrust has led to privacy as a public good coming to fruition in the Covid-19 response across Europe, whereas compliance has remained the dominant norm in Latin America.

While there are some areas of convergence and shared issues – in particular about the lack of decentralized systems, about the anonymity of data, the compliance with data protection regimes, and lack of protections for personal data seen in some apps – especially as outlined by the Chaos Computer Club, the Open Rights Group, and the Karisma Foundation, the prominence of these concerns, and the influence of the organisations highlighting them has a very different impact depending on the country in which the concerns are raised. The key message that must be taken away from this analysis therefore rests at odds with the international community approach to privacy, data protection, and human rights, and suggests that while there must

[86] Gonzalo Salano, 'Ecuador uses technology to fight COVID-19' (*AP,* 16 April 2020) <https://apnews.com/516d5ddc49e3436c8681356a640c6a46> accessed 22 July 2020.

remain an emphasis on protecting rights and data, and aspiring to benchmarks must be the overarching goal, there is no one size fits all approach.

The national traits and characteristics of states in Latin America are very different to those in Europe – privacy and data protection are recognised concerns, but they are not the dominant ones that set the agenda in Colombia and Ecuador, and other factors take the lead. One major obstacle is the lack of interoperability across apps from different countries, making the international tracing effort even more difficult. The cross-border use of tracing apps also poses problems as lockdown restrictions are lifted – notably due to the enforcement of data protection and privacy rights, but also because of the lack of interoperability across apps and national borders. The regulation of such apps is an apparent afterthought, especially given the speed with which such tracing systems have been rolled out.

Undoubtedly, there is best practice – i.e. a regional consensus in responding to Covid-19 through the collection of data, and the use of a smartphone app to allow real time information to be gathered by decision makers – in establishing a tracing app to respond to Covid-19. Similarly, the work of civil society and NGOs in scrutinising the apps in various nations is vitally important and provides the core analysis of the scope of the data to be collated and retained. Without the work of these organisations, and their coming together internationally to share their research and expertise, it would be much more difficult to ascertain any kind of benchmarking for track and trace apps in different legal and regional areas. The holding to account of tracing systems and governments in utilising technology that is by its very nature invasive is vital in protecting rights. In times of crisis in particular, accountability is incredibly important to ensure that digital rights are not pushed aside in light of other concerns.

Much of the reporting of the tracing apps, tracking programmes, and privacy concerns during the developmental processes and the initial stages of the pandemic have focussed on pitting digital rights and privacy against public health interests. The two are not mutually exclusive and yet the media suggest that they cannot coexist.[87] Such attitudes must change, and a balance must be struck. In attempting to balance digital rights and privacy, and public health, accountability and transparency are essential – the scrutiny of the track and trace systems in Germany, the UK, and Colombia indicates exactly this. The overwhelming conclusion is that privacy, digital rights, and human rights concerns abound – the Karisma Foundation, Chaos Computer Club, and Open Rights Group have all outlined significant – and shared – concerns in different countries over fundamentally different apps with a similar function.

It is increasingly appropriate to use anonymised health data to identify clusters of disease, so the use of tracing is not new. However, the concerns surrounding transparent, trustworthy ways of doing so persist. A greater emphasis is falling on

---

[87] Emily Sharpe, ‘Using data to fight Covid-19 does not mean lowering the bar for privacy’ (*Web Foundation*, 15 June 2020) <https://webfoundation.org/2020/06/using-data-to-fight-covid-19-does-not-mean-lowering-the-bar-for-privacy/> accessed 22 July 2020.

uses of data, but the privacy concerns – and the evolving norms in pursuing privacy as a public good remain a matter of national and regional disconnectedness. We should be using data to fight Covid-19, but we should not be setting privacy aside.