Applied Ethics and Digital Information Privacy: Informing the Design of Covid-19 Contact Tracing Apps

Kathrin Eismann
University of Bamberg, Germany

Diana Fischer-Preßler
University of Bamberg, Germany
diana.fischer-pressler@uni-bamberg.de

Kai Fischbach
University of Bamberg, Germany

Abstract

To counteract the spread of Covid-19, many countries have introduced mobile applications for contact tracing, which raises considerable questions about how these apps protect users' information privacy. Through an exploratory analysis of Covid-19 contact tracing apps being used in Australia, France, Germany, Japan, and New Zealand, we identify normative and technical principles for the design of privacy-sensitive contact tracing apps. Based on a Restricted Access/Limited Control (RALC) account of information privacy, we discuss how the apps protect users' information privacy through limiting access to and allowing users to actively manage their personal information. Our findings illustrate what understanding of information privacy is evident from the various designs of Covid-19 contact tracing apps, and how competing design principles can contribute to users' information privacy. From a practical perspective, our findings can inform the design of contact tracing apps and the development of privacy approaches that can be applied in particular contexts. Our work thus bridges the gap between ethical design guidelines and technical analyses of specific implementations.

Keywords: applied ethics, disclosive computer ethics, information privacy, mobile app, contact tracing, coronavirus, Covid-19, crisis, pandemic, normative theory.

1 Introduction

The coronavirus pandemic has confronted public health officials throughout the world with the urgent need to contain infections and stop the spread of the highly contagious and harmful Covid-19 disease. As it spread across the globe, borders were closed, social and economic life came to a standstill, and health infrastructures nearly collapsed. Almost a year into the pandemic, neither medication nor vaccinations were available; in February 2021, the World Health Organization (WHO) had registered more than 105 million cases and more than 2.2 million fatalities due to Covid-19 worldwide (WHO, 2021b).

To counteract further spread of the virus and prevent sustained economic damage and the loss of human life, public health interventions through which people can avoid exposure to the coronavirus—such as *cordons sanitaire*, traffic restrictions, and social distancing—have gained momentum (e.g., Di Gennaro et al., 2020, Pan et al., 2020). Beyond that, the WHO has established *contact tracing* as a key strategy for interrupting transmission chains, as people who have been in contact with an infected person can be identified and advised to quarantine to prevent further transmissions (WHO, 2021a).

However, classical procedures for identifying the contacts of an infected person can be ineffective, if, for instance, a person's contacts are unknown or low levels of automation cause delays in the identification and contacting of people at risk (WHO, 2021a). Therefore, governments have considered, and some have implemented, mobile applications—so-called *contact tracing apps*—to trace infections and provide health advice to citizens. Mobile applications reduce reliance on human recall and hence can be more effective than classical procedures for contact tracing, especially in densely populated areas with high degrees of mobile connectivity (Budd et al., 2020). These digital tools were thus ascribed an important role in limiting the propagation of the pandemic (WHO, 2021a).

Contact tracing apps are applications that run on a smartphone and allow tracing encounters between users. They are a technical approach to tracking epidemic chains of infection and stopping the spread of Covid-19. Basically, they are used to alert users who have been in contact with another infected user, but may not (yet) show typical symptoms of the Covid-19 disease. Those users can then be advised to self-isolate and get tested. Users receive a warning via the app that they might be at risk of an infection if they have been close (e.g., within a couple of meters) to another user diagnosed with Covid-19 if that proximity was for an epidemiologically relevant time interval (e.g., 15 or more minutes) within a relevant timeframe (e.g., an estimated incubation period of 14 days for the infected person). Users so warned can then seek medical advice and take appropriate action. If they are themselves diagnosed with Covid-19, they can update their status within the app so others who have been close can also receive warnings (Ahmed et al., 2020).

To enable effective tracing, however, apps need to collect sensitive personal data, which includes records of users' health, movements, and social interactions (Morley, Cowls, Taddeo, & Floridi, 2020). Experts warned early on that personal information collected through contact tracing apps could be exposed to a number of security risks that threaten user information privacy. Privacy could be compromised due to, for instance, technical problems or cyberattacks, potential misuse of personal data due to large-scale social surveillance, and illegitimate repurposing of the information collected (e.g., Klar & Lanzerath, 2020). Concerns over data protection and information privacy norms could negatively affect people's intention to use these apps (e.g., Chan & Saqib, 2021, Fischer, Hattori-Putzke, & Fischbach, 2019; Fodor & Brem, 2015), which, in turn, could lower the efficacy of app-based contact tracing (Trang, Trenz, Weiger, Tarafdar, & Cheung, 2020).

Several guidelines have been developed, both by researchers (e.g., Floridi, 2020; Klar & Lanzerath, 2020) and public health institutions (e.g., European Commission, 2020; WHO, 2020), to promote the design of apps for Covid-19 contact tracing that preserve users' information privacy. Still, analyses suggest that despite government claims to honor citizen information privacy, several apps have failed to meet essential requirements of privacy-sensitive design (e.g., Hatamian, Wairimu, Momen, & Fritsch, 2021, Woodhams, 2020). Clearly, the risk of information privacy violations cannot be eliminated through technical implementation alone, but relies on a shared understanding of what constitutes information privacy violations through illegitimate access and use of personal information.

Our work bridges the gap between ethical design principles for and technical evaluations of Covid-19 contact tracing apps. Based on the *Restricted Access/Limited Control* (RALC) framework of information privacy (Moor, 1997; Tavani & Moor, 2001), we evaluate the normative and technical design principles that have—explicitly or implicitly—guided the

development of apps deployed as early as during the second half of 2020 in five liberal democracies. Our analyses are based on two complementary research questions:

RQ1: What normative and technical design principles to protect information privacy are evident from Covid-19 contact tracing apps?

RQ2: What understanding of information privacy is evident from the design of Covid-19 contact tracing apps?

Going beyond purely normative approaches, we establish a frame of reference that explicates standards of privacy-sensitive design from the perspective of real-world mobile applications, thus emphasising principles that are both technically applicable and in line with the ethical standards of liberal democracies. In contrast to mere technical analyses, we elaborate how the identified design principles relate to ethical information-privacy requirements, and discuss how they might contribute to the achievement of normative goals.

Our research approach is one of *explicit morality* (Stahl, 2012), as we explicate the normative understanding of information privacy that is evident from the design of existing Covid-19 contact tracing apps. Thus, we aim to clarify what users can expect with respect to the protection of their personal information when using these apps. While developing full-fledged ethical theory is beyond the scope of this paper, we identify normative and technical design principles that can guide the design of technical artifacts that allow large-scale collection of sensitive personal data. Finally, our work demonstrates how concepts of normative theory can be analysed based on empirical design choices, which can encourage researchers to abstract information privacy conceptualisations and possible breaches within a certain artifact under investigation and evaluate alternative solutions in terms of how they afford information privacy.

We apply *disclosive computer ethics* to analyse information privacy conceptualisations evident from existing Covid-19 contact tracing apps, as described by Brey (2000a, 2000b). Key to our work is the assumption that while the apps have been designed to preserve information privacy in line with pertinent laws and social norms (e.g., European Parliament, 2020), their design and other features determine the extent of information privacy when using the apps. Based on an exploratory analysis of information-privacy principles evident from the five apps, we evaluate how the measures implemented relate to normative and technical protections of information privacy, as conceptualised by the RALC framework, and discuss how normative theory can hence guide the design of privacy-enhancing artifacts.

Below, we briefly delineate the theoretical notion of information privacy that underlies our work, and how Covid-19 contact tracing apps might violate it. Furthermore, we explain how normative and technical design principles, according to the RALC framework, could help protect information privacy. On that basis, we describe our research methodology and the findings of the exploratory analysis and theoretical evaluation, and discuss the theoretical and practical implications of our work.

2 Information Privacy in the Context of Covid-19 Contact Tracing Apps

Information privacy is a subset of general privacy (Bélanger & Crossler, 2011) that refers specifically to personal information (Smith, Dinev, & Xu, 2011), which, in turn, implies "facts about a person which most individuals … do not want widely known about themselves"

(Parent, 1983, pp. 269-270). In a normative sense, information privacy is one of liberal societies' key moral values, whereas in a descriptive sense, it refers to a quality of a situation that can be present or absent (Becker, 2019). Thus, information privacy comprises "the claims of individuals that data about themselves should generally not be available to other individuals and organisations, and that, where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use" (Clarke, 1999, p. 60).

Digitally enhanced means of information sharing and communication are widely believed to threaten people's information privacy, especially because they enable constant and unobtrusive monitoring and profiling (Becker, 2019). They make it easy to record, analyse, and share personal information about users, retain it for an indefinite time, match it with data from secondary sources, and thus generate novel and possibly revealing insights about users (Nissenbaum, 1998). In addition, they may incentivise users to contribute additional information about themselves to facilitate interactions (Volokh, 2000)—a condition commonly known as the "commodification of privacy" (Campbell & Carlson, 2002).

Information privacy is only one among several ethical issues that require consideration with Covid-19 contact tracing apps (Floridi, 2020). In fact, Blasimme and Vayena (2020, p. 761) conclude that most of these apps "are built with a proactive commitment to privacy-preserving technological features (privacy by design) and only use strictly necessary data (privacy by default)." Existing Covid-19 contact tracing apps have typically been developed with an explicit commitment to pertinent privacy laws and regulations; many, if not most, have been subjected to intensive public debate and scrutiny to enhance their compliance with commonly shared social norms (e.g., European Parliament, 2020).

Still, the risk of misuse and vulnerability of personal information collected on a large scale (e.g., due to hacking or cyberattacks) remains (Klar & Lanzerath, 2020). Furthermore, absent evidence on the efficacy of the apps, users' information privacy may be threatened by a lack of proportionality, as well as the risk of function creep if the data collected through the apps is repurposed, potential ignorance of sunset clauses and continued use of the apps even after the Covid-19 pandemic is declared contained, and the risk of unrevealed non-voluntariness if social or economic conditions render the use of the apps obligatory in some *de facto* way (Ishmaev, Dennis, & van den Hoven, 2021). Furthermore, information privacy risks arise in cases where malevolent users can infer from the app who may be infected, state-level agents or service providers can access personal user information illegitimately, or if such information is leaked due to negligence or malicious attacks (Boutet et al., 2020). Rowe (2020) also observes that governments tend to overemphasise the potential short-term benefits of using Covid-19 contact tracing apps, while downplaying long-run threats to information privacy.

Covid-19 contact tracing apps can threaten users' information privacy in two fundamental ways: they can interfere with users' ability to control access to their personal information (*privacy as control*); and they can facilitate the access by others to personal information about a user in a given situation *(as a state*). While the former defines information privacy in terms of the ability of agents to control access to information about themselves, the latter understands it as a condition in which access to personal information is limited to some extent (Smith et al., 2011). Both conceptions of information privacy have their roots in historical privacy theories, and both come with a number of theoretical virtues and drawbacks (Tavani, 2007, 2008). However, understanding information privacy merely in terms of control is problematic when

agents deliberately relinquish control over information about themselves (Tavani & Moor, 2001).

In the *Restricted Access/Limited Control* (RALC) framework of information privacy, by contrast, Moor (1997) and Tavani and Moor (2001) define information privacy primarily in terms of limited access to personal information. They recognize that while perfect control over personal information may be impossible when it comes to digital information and communications technologies, people should be able to rule out undesired access to and use of information about themselves. The RALC framework integrates two elements: the *condition of privacy*—the extent to which information privacy is present in a particular situation, and which relies on the absence of access to personal information; and the *management of privacy*—people's ability to determine who can access information about them for what purpose and in what ways, which requires that information subjects have control over their personal information. Through actively managing access to personal information, agents are hence assumed to determine the amount of information privacy in a given situation.

According to the RALC framework, information privacy is a characteristic of situations in which people are normatively protected from intrusion, interference, and information access by others. Situations are the key unit of the RALC framework; they can comprise locations, relationships, and activities. Situations can be *naturally private*, meaning there are natural or physical circumstances that protect people from intrusion or observation. In naturally private situations, privacy exists as a matter of fact. When others gain access to information about a person in such situations, that person's privacy is lost but not violated, as they do not have a normative claim to it. In contrast, in *normatively private* situations, personal information is protected through norms that determine who may access it. These norms constitute a person's right to privacy in a particular situation; privacy is violated only when pertinent norms are trespassed (Moor, 1997; Tavani & Moor, 2001).

RALC introduces three mechanisms of individual control through which actors can achieve an adequate level of information privacy, although they do not constitute a right to privacy beyond what is granted by situational norms: *choice* over situations that offer the desired level of information privacy; *consent* to give up the right to information privacy in a particular situation; and *correction* of personal information collected (Tavani & Moor, 2001).

Just as in the case of offline social relations, interactions enabled by digital information and communications technologies can constitute situations (Tavani, 2007). Thus, from a RALC perspective, using a contact tracing app can constitute both a naturally and a normatively private situation, depending on the context of app use and the specific design of the app. While pertinent social and legal norms and a shared understanding that users must somehow be able to determine to whom their personal information is made available are the basis for normative protection of their information privacy, it is the app's technical features that determine the extent to which users are actually protected from intrusion, and hence render app usage naturally private. Figure 1 illustrates how the use of Covid-19 contact tracing apps can be interpreted within the RALC framework.

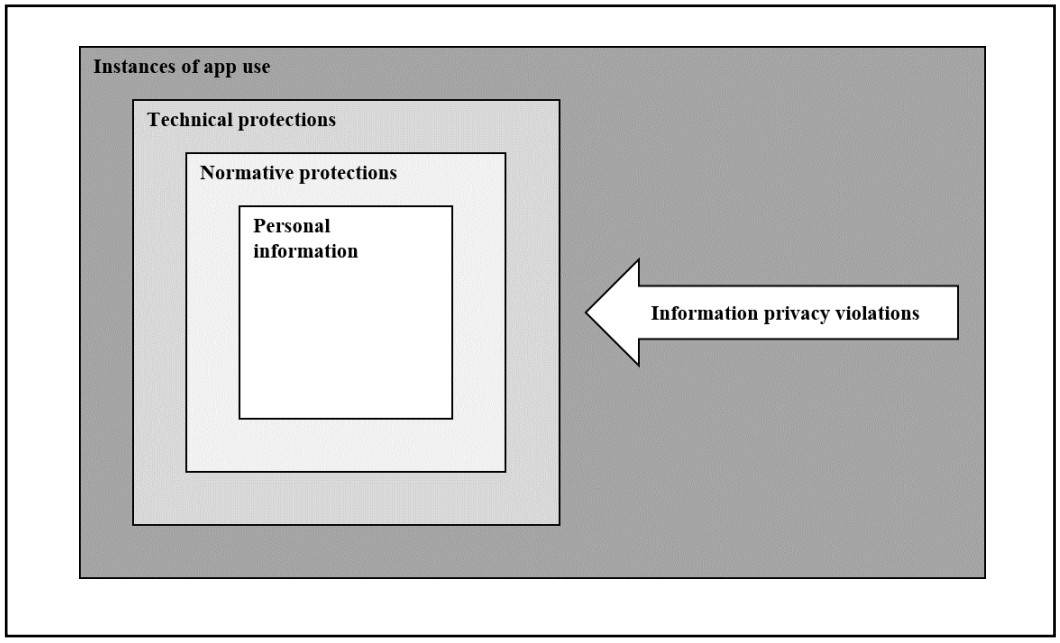

Figure 1. A RALC perspective on information privacy in the context of Covid-19 contact tracing app use.

In our work, it is instances of app use that constitute the situations to be analysed. Those are characterised by two key attributes: *personal information* that is exposed to potential information privacy violations, and the *information privacy violations* that potentially apply. Personal information is embedded within two layers of protection. The first layer is *normative protections of information privacy*, which consists of norms—broadly defined as principles of action that specify appropriate behaviour in a given society—that determine what information about users may be legitimately accessed through the app, by whom, and under what conditions. Access to personal information contravening these norms is considered to violate users' information privacy. The second layer is *technical protections of information privacy*, which comprise the particular technical features through which personal information is protected from unwarranted access. These constitute natural barriers in the RALC terminology: they do not grant users a normative right to information privacy, but nevertheless can be effective in preventing access to their personal information.

Below, we explain how we have analysed these key elements of existing Covid-19 contact tracing apps, following a disclosive research approach, and elaborate on what our insights reveal about the understanding of information privacy that is evident from the apps' design.

3 Research Methodology

3.1 Disclosive Computer Ethics

In our research, we have followed the tenets of disclosive computer ethics, assuming that technological artifacts are not morally neutral, but may have hidden moral properties that can be uncovered through disclosive analysis (Brey, 2000a, 2000b). Basically, technological artifacts are assumed to serve as mechanisms that constrain people's individual and social behaviors, and hence can enforce or promote normative action (Brey, 2000b).

Studies in disclosive computer ethics require a two-step approach. Relying on an inductive approach, in the first step, a technological artifact is analysed from the perspective of some

moral value to draw preliminary conclusions regarding the relationship of the artifact's features to the moral value of interest. Then, in the second step, moral theory can be applied to evaluate more specifically the artifact's normatively relevant features and properties, which also creates the potential for further developing existing theory (Brey, 2000a, 2000b).

Below, we explain how we have analysed the normative and technical design principles that determine how the technological artifacts in our work—mobile apps for Covid-19 contact tracing—protect information privacy, based on the RALC framework delineated above.

3.2 Case Selection and Data Acquisition

Our analyses are based on Covid-19 contact tracing apps from five liberal democracies (according to Freedom House; Repucci & O'Toole, 2020) that released the apps for their residents to use as early as the second half of 2020: Australia, France, Germany, Japan, and New Zealand. We selected these countries because they provide early examples of privacy-sensitive design for Covid-19 contact tracing apps (as opposed to digital tools applied for other purposes, such as outbreak detection and case identification; Budd et al., 2020) against a somewhat comparable socio-political background.

These countries' governments have all stated that the apps comply with national privacy laws and regulations, and were designed especially to meet pertinent norms of information privacy. In the European Union, for instance, the ROBERT (ROBust and privacy-presERving proximity Tracing) protocol was established to facilitate developing privacy-preserving contact tracing apps in line with the pertinent General Data Protection Regulation (GDPR), and governments have established *a priori* guidelines to guide that work (e.g., European Parliament, 2020). The approaches taken to protect information privacy, however, vary. This *purposive sample* of Covid-19 contact tracing apps thus allows us to draw conclusions about the implementation of information privacy concerns in liberal democracies based on cases with maximum possible heterogeneity at the time. Table 1 is an overview of the apps analysed.

The five apps we studied are applications for contact tracing that analyse physical contacts between people, using Bluetooth, for instance, to measure the distance between smartphones on the basis of signal strength and thus detect potential encounters between users (i.e., *proximity tracing*). Unlike other mobile apps that track people's geo-locations (i.e., *tracking apps*), proximity tracing apps cannot be used to create detailed movement profiles to monitor people's behaviors, for instance, to ensure compliance with quarantine orders. While both involve sensitive data, privacy concerns for the two types of applications differ, and proximity tracing apps are considered, by design, to be more privacy-sensitive (Taddeo, 2020) and also more compatible with privacy expectations in liberal democracies than tracking solutions that have been used in South Korea, Taiwan, and Israel, among other countries (Zastrow, 2021).

We downloaded the official documentation provided by the institutions in each country responsible for the development, infrastructure, and service provision of the apps (date of reference: 2020-06-30). We analysed English versions of the documents, using machine translations (*Google Translate*) when English texts were not available.

Country (app name)	**Description**	**Responsible institutions**	**Information sources used**
Australia (COVIDSafe)	• To use the app, users must register and provide personally identifying information that is used to contact them in case they are at risk of infection; the information is stored on a central server. • Within the app, each user is represented by an automatically generated ID that changes at regular intervals to prevent users from inferring their own or others' IDs. • The app uses Bluetooth to detect other users nearby. In case of an encounter, it saves these users' IDs, the date and time of contact, phone model, and Bluetooth signal strength. • Infected users are notified by human contact tracers and asked to upload their encounter information to a central server. If they consent to do so, they receive a PIN to authorise the transmission. • Contact tracers then use the encounter information and personal ID information of other users to identify and prioritise persons who may have been in contact and advise them of their risk status.	Australian Government Department of Health	Australian Government, 2020; Australian Government Department of Health, 2020
France (StopCovid)	• Once installed, the app creates a unique identifier that represents the user. • The app uses Bluetooth to detect other users nearby. In case of an encounter, it saves these users' IDs, the date and time of contact, and the inferred distance between users based on Bluetooth signal strength. • Infected users receive a QR code or similar proof from public health services, which they can use to update their health status within the app. • If they update their status, the infected user's encounter history is uploaded to a central server and warnings are sent to the devices of other users for whom an encounter was registered.	Ministry of the Economy, Finance and Recovery	Inria, 2020a, 2020b, 2020c; Ministére De L'économie des Finances et de la Relance, 2020a, 2020b
Germany (CoronaWarn)	• Each user is represented within the app by an automatically generated ID, which changes at regular intervals to prevent users from inferring their own or others' IDs. • The app uses Bluetooth to detect other users nearby. In case of an encounter, it saves these users' IDs, the date and time of contact, and the inferred distance between users based on Bluetooth signal strength. • Infected users receive a QR code or similar proof from public health services, which they can use to update their health status within the app. • If they update their status, the infected user's ID is uploaded to a central server, which in turn makes it available to others' devices, which compare it with those users' own encounter histories and generate warnings if they have registered an encounter with the infected user.	German Federal Government	Corona Warn App Open Source Project, 2020; The Federal Government, 2020a, 2020b

Country (app name)	Description	Responsible institutions	Information sources used
Japan (COCOA – COVID-19 Contact)	• Each user is represented within the app by an automatically generated ID, which changes in regular intervals to prevent users from inferring their own or others' IDs. • The app uses Bluetooth to detect other users nearby. In case of an encounter, it saves these users' IDs, the date and time of contact, and the inferred distance between users based on Bluetooth signal strength. • Infected users can register with their email address or phone number to receive a processing number from public health services, which they can use to update their health status within the app. • If they update their status, an infected user's ID is uploaded to a central server, which in turn makes it available to others' devices, which compare it with those users' own encounter histories and generate warnings if they have registered an encounter with the infected user.	Ministry of Health, Labour and Welfare	Ministry of Health, Labour and Welfare, 2020a, 2020b
New Zealand (NZ COVID Tracer)	• Users must sign up with their email addresses to use the app. They can add further personally identifying information to their profiles. • The app allows users to keep a digital diary of locations visited, which they can enter by scanning QR codes or manually adding entries of places, activities, dates, and times visited. • Users who are confirmed or deemed likely to be infected are notified by contact tracers to upload their location history to a central server. • If they update their status, human contact tracers evaluate the location history and identify locations at which persons in contact with an infected user would have been at risk of infection. These locations are made available to users' devices, which in turn generate warnings if they detect a match between their own location entries and a relevant exposure location and timeframe.	Ministry of Health	Ministry of Health, 2020a, 2020b

Table 1. Overview of Covid-19 contact tracing apps

3.3 Exploratory Analysis

Following from the RALC framework (Moor, 1997; Tavani & Moor, 2001), we understand information privacy in terms of limited access to information about a person, with the subjects of the information being able to determine by whom, in what ways, and to what end that information is accessed and used. This definition is thus in line with prior research in information systems (Smith et al., 2011), but also broad enough to encompass different understandings of what information is subject to privacy concerns, what constitutes unwarranted access to and use of personal information, and how apps can be designed to protect user information privacy.

We used a multistage qualitative coding procedure to analyse the apps. In the first stage, we identified statements that referred to personal information about users from each app's documentation. In the second stage, we used these statements to develop inductive codes that

describe what information about app users was specified as collected or not collected, what kind of access to or use of that information might violate user information privacy, and what normative and technical design principles were applied to afford information privacy protection. In the third stage, we summarised these descriptive codes into coherent categories, which we describe in the following section. Two of the paper's authors undertook qualitative coding, with one in charge of each coding stage and the other reviewing and revising the codes. Disagreements were resolved through consensual discussion.

Below, we summarise our findings on the types of personal information collected by these Covid-19 contact tracing apps, the violations of user information privacy accounted for, and the different approaches to preventing violations spelled out in the documentation.

4 Results of the Exploratory Analysis of Covid-19 Contact Tracing Apps

4.1 Personal Information Collected

The Covid-19 contact tracing apps we studied collect different types of personal information: *person identifying information* that allows for identifying a particular person who may be using the app (i.e., users and other persons about whom information is collected through the app); *user identifying information* that allows for identifying a particular user or device on which the app is installed; *encounter information* about contacts between users through which Covid-19 might be transmitted; *user profile information* about user preferences and activities using the app; and *health status information* about a user's actual or potential Covid-19 infection. Table 2 provides an overview of the types of personal information collected by the analysed apps.

Only the Australian app requires users to enter a name, age range, postal code, and contact phone number to facilitate tracing. The New Zealand app allows users to enter personal details and information about their social contacts to identify other people who might be at risk; users must also provide an email address to complete the registration. The French and Japanese apps require an email address or mobile phone number so infected users can receive a verification code to authorise health status updates that indicate they have become infected. The German app does not collect person identifying information.

Both the Australian and the New Zealand apps collect information that can be used to trace individual users. The Australian app registers the model of the smartphone on which the app is installed, and the New Zealand app asks users to enter information about their locations and activities to detect potential encounters. In contrast, the French, German, and Japanese apps stress that no information is collected that would enable identifying the user or the device on which the app is installed. None of the analysed apps collects geolocation information.

In addition to person and user identifying information, all the apps except the New Zealand app create unique identifiers for each user. These are linked to the records of users' previous encounters and are exchanged between nearby devices to constitute encounters; they use Bluetooth to record the dates, times, and estimated duration of encounters and proximity of contact based on Bluetooth signal strength. The New Zealand app does not record encounters directly; rather, it allows users to keep a digital diary of places they have visited and infers from that possible encounters with other users who have checked in at the same location at the same time.

Countries	AUS	FRA	DEU	JPN	NZL
Person identifying information					
Name	X				
Age range	X				
Post code	X				
Phone number	X	X		X	
Email address		X		X	X
Social contacts					X
User identifying information					
Device model	X				
Location					X
Activities					X
Encounter information					
Date and time	X	X	X	X	X
Spatial proximity	X	X	X	X	
Duration of contact	X	X	X	X	
User profile information					
User identifier	X	X	X	X	
Encounter history	X	X	X	X	
User interests					X
Health status information					
Positive test result	X	X	X	X	X
Risk status (binary)		X	X	X	
Risk status (qualitative)	X				X
Health record				X	

Table 2. Personal information collected by Covid-19 contact tracing apps

Finally, all the apps allow users to update their health status if they have tested positively for Covid-19. This information is then combined with encounter information to evaluate users' risk status and issue warnings accordingly. Estimated risk status can be binary, as in the French, German, and Japanese apps—that is, the app differentiates only between users who are at risk of infection (because they have been close to an infected user for an epidemiologically relevant period) and those who are not. The Japanese app allows users who have received a warning to enter further information about their health status and possible symptoms so they can be provided with more tailored advice.

The Australian and New Zealand apps allow for more detailed qualitative risk assessments. Risk status with the Australian app is evaluated by human contact tracers, who get in touch with users who might be at risk of infection based on their encounter information and other information, such as the number of encounters, duration of contact, and estimated distance between users during an encounter. For the New Zealand app, contact tracers evaluate the locations at which an infection was likely to occur, and issue warnings selectively to persons potentially at risk.

4.2 Accounting for Potential Information Privacy Violations

The Covid-19 contact tracing apps we studied account for three broad types of information privacy violations: *illegitimate acquisition of personal information* without a justified cause or in an unjustified way; *misrepresentation of personal information* respectively users based on information that is collected by the app but does not accurately describe the user or their condition; and *misuse of personal information* by processing or utilising it in an unjustified way or for an unjustified purpose. Table 3 is an overview of information privacy breaches for which

we found precautions spelled out in the official documentation of the analysed Covid-19 contact tracing apps.

Countries	AUS	FRA	DEU	JPN	NZL
Illegitimate acquisition of personal information					
Forced use of the app	X	X	X	X	X
Forced self-disclosure	X	X	X	X	X
Uneconomic data collection		X	X	X	
Prolonged data collection	X	X			
Misrepresentation of personal information					
Unauthorised registration and use of the app	X				X
Misreporting personal information	X	X	X	X	X
Misuse of personal information					
Illegitimate access	X	X	X	X	X
Aggregation		X			
Recombination		X	X	X	
Repurposing	X		X	X	X

Table 3. Information privacy violations accounted for by existing Covid-19 contact tracing apps

The institutions responsible for all five apps agree that installation and use of the app must be voluntary. Furthermore, they state that users must not be forced to provide any personal information. In particular, they must not be obligated to provide information about their health status, disclose test results within the app, or share any personal data with health authorities or other agents.

In the documentation for the French, German, and Japanese apps, collecting data beyond what is absolutely necessary and relevant to enable contract tracing is considered a violation of users' information privacy. For the Australian and French apps, prolonged data collection beyond the duration of the coronavirus pandemic is characterised as a potential breach of information privacy.

The documentation also accounts for the fact that misrepresenting users based on the personal information collected could potentially threaten the integrity of the apps, and so information collected must be accurate, complete, and up to date. For the French, German, and Japanese apps, this refers in particular to encounter information and information about a user's health status and test results—users are encouraged to submit timely information about positive test results. False reports regarding positive tests for Covid-19 are prevented by enabling the update of the infection status only through a code provided by the responsible health institution. The documentation for the Australian and New Zealand apps states that misrepresenting person or user identifying information that is used to identify potential contacts is not approved.

The accompanying documentation for all five apps addresses illegitimate access to personal information as a violation of information privacy: other app users, service providers, health authorities, and third parties are not allowed unauthorised access to personal information, nor may this information be made available or transmitted to them. In addition, the French app's documentation explicitly forbids data aggregation, which means personal information must not be accumulated in a way that allows clustering of users based on that information (e.g., compiling lists of infected users). The French, German, and Japanese apps further prohibit the recombination of personal information—that is, associating or matching personal information

to make inferences about other users' personal attributes (e.g., their health status or social contacts). Finally, the documentation for all but the French app discourage the use of personal information provided through the app for purposes other than Covid-19 contact tracing (e.g., preventing access to restaurants and other facilities, or monitoring user compliance with quarantine orders), although data are generally used to provide use statistics and improve app functionality. While we expect that the same holds true for the French app, we were not able to identify corresponding statements in the documentation.

4.3 Design Principles to Protect Users' Information Privacy

The analysed apps are based on several design principles aimed at protecting personal information from illegitimate access and use. These include *voluntarines*s, that is, no one is compelled to install or use the app or add personal data, any information entered can be deleted, and the app can be uninstalled at any time. The apps are based on t*ransparency* that makes the manner in which the app collects and uses personal information known to users. *Data minimisation* ensures that only data that are absolutely necessary and relevant for contact tracing are collected. The app design can include *pseudonymisatio*n—only user-chosen or automatically generated pseudonyms are used to refer to users. The *protection of personal information* from unwarranted access by users and others is part of the apps' design and, finally, can enable users to verify, review, and correct their personal information. Table 4 is an overview of the design principles through which the analysed Covid-19 contact tracing apps seek to prevent violations of information privacy.

To implement the principle of voluntariness, the adoption and use of all analysed apps is left to people's discretion: neither governments nor other agents may force or otherwise exert pressure on people to install the apps. Further, providing personal information within the apps—particularly about a user's health status and a potential Covid-19 infection—is optional. Users may uninstall the app at any time, and doing so will delete all personal information stored on their devices; if information pertaining to them is stored on some central server, they can request its deletion.

All the responsible institutions emphasise transparent design. Privacy information is made available to users both within the app and online. Applicable privacy laws and regulations are explicitly referenced, and contacts for privacy-related inquiries are provided. Furthermore, governments have approved the design of the apps, either implicitly or explicitly; for instance, French and German government and civil agencies responsible for information privacy and data protection were involved in their country's app development to ensure compliance with privacy standards. Furthermore, the French and German apps are open source, meaning the source code and technical specifications of the apps are publicly available, and community members and external experts are encouraged to review and comment on the code.

The French, German, and Japanese app documentation strongly emphasises minimisation with respect to data collection. These apps do not require user identifying information to be entered to use the app, and only minimal person identifying information is required for the setup. Furthermore, they impose quantitative thresholds on data collection, which implies that encounters are recorded and stored only when some threshold values in proximity and duration are exceeded (less than 1 meter for 15 minutes or more for the French and Japanese apps, and more than 10 minutes for the German app). Both the Australian and the New Zealand app documentations, in contrast, emphasise data richness to allow for graded risk

assessment. While they do not track user geolocations, both collect data that could be used to identify particular users.

Countries	AUS	FRA	DEU	JPN	NZL
Voluntariness					
Voluntary use of the app	X	X	X	X	X
Voluntary self-disclosure	X	X	X	X	X
Discontinuance of use	X	X	X	X	X
Transparency					
Transparent privacy standards	X	X	X	X	X
Government approval	X	X	X	X	X
Agency involvement		X	X		
Open source development		X	X		
Data minimisation					
Qualitative data collection thresholds		X	X	X	
Quantitative data collection thresholds		X	X	X	
Temporally restricted storage	X		X	X	
Discontinuance of service provision	X	X			
Data protection					
Encrypted storage	X	X	X	X	X
Decentralised storage			X	X	X
Centralised storage	X	X			
Restricted device-to-device transmission	X	X	X	X	X
Secure transmission			X	X	
Pseudonymisation					
Personal pseudonyms	X				
Random user identifiers	X	X	X	X	
Dynamical user identifiers	X		X	X	
Logical disconnectedness		X	X	X	
Data quality enhancement					
Technical redundancies		X	X	X	X
Verification	X	X	X	X	X
Revision	X				X

Table 4 Principles to protect users' information privacy in Covid-19 contact tracing apps

The Australian, German, and Japanese apps store encounter information only for a limited period (14 days for Germany and Japan; 21 days for Australia). While we cannot rule out the possibility that the other apps impose similar restrictions, we were not able to confirm that based on official documentation. Furthermore, the Australian and French apps, according to official announcements, are to be discontinued at the end of the Covid-19 pandemic, including automatic deletion of all personal information stored. We were not able to identify similar statements regarding the other apps.

Pseudonymisation is another measure taken to protect users' information privacy. The Australian app allows users to enter false names or self-chosen pseudonyms upon registration. Other apps employ user IDs that are generated automatically within the app and are linked to user digital profiles, which allows for retracing a user's encounters. With the exception of the New Zealand app, all apps analysed use these randomly generated identifiers. The accompanying documentation for the Australian, German, and Japanese apps also state that

these identifiers change at regular intervals to prevent users from identifying nearby other users or retracing infected users.

Documentation of the apps also stresses that user pseudonyms are logically disconnected from other pieces of personal information, which means they are inherently unrelated. For instance, in the French, German, and Japanese apps, user identifiers are generated randomly and are not based on any person identifying information. Similarly, the codes that users enter to verify test results are independent of these identifiers, so servers or users' devices can only know that some user has tested positively for Covid-19, but cannot infer that user's identity. While the Australian app also uses randomly generated identifiers for exchanges between users, those are connected to person identifying information made available to contact tracers, which means they can infer the identity of infected or potentially infected users. Similarly, for the New Zealand app, contact tracers know the identities of infected users, although they cannot directly identify users at risk. None of the apps provides real-time alerts, which means that the apps cannot be used to detect infected persons in a user's proximity.

For all apps, encrypted storage is key to protecting personal information from unwarranted access. Apps differ, however, in their data storage models: the German and Japanese apps use decentralised storage of personal information, which means that as little information as possible is transmitted from the individual users' devices to central servers. Instead, the identifiers of infected users are uploaded so other devices can compare them with their own encounter histories. Similarly, users of the New Zealand app who have tested positive for Covid-19 can upload their location histories so that warnings can be generated for particular locations and other users' devices can compare their own entries. The French app, in contrast, asks infected users to upload their encounter histories; each device knows only its own encounters, and matching is performed on a central server. The Australian app relies even more on a central server infrastructure: upon registration, users provide person identifying information, which is stored centrally. In case of an infection, users are asked to upload their encounter histories, and both sources of information are matched by human contact tracers to identify and prioritise contacts.

Secure transmission between devices and servers can be an issue, although only the German and Japanese app documentation refers explicitly to secure device-to-server transmission, and only the latter mentions prospective security measures to obscure transmissions (e.g., sending false notifications that are discarded on the server to create background noise).

Both storage models are generally motivated in terms of information privacy concerns. Decentralised storage, on the one hand, minimises the threat that health agencies or service providers can access personal information stored on a central server, or that sensitive data could be released unintentionally if servers are compromised. Centralised storage, on the other hand, can hinder individual users from accessing user identifying information (e.g., their identifiers), reduces information privacy risks from smartphone security holes and loss or theft of devices, and allows for bundling the responsibility for data protection with one or a few dedicated agents. Decentralised storage does not imply that no personal information is transmitted to a central server; at the very least, all apps that rely on this approach use central servers to verify test results and make the identifiers of users diagnosed with Covid-19 available to others' devices. Similarly, centralised storage does not mean that no information is stored on users' devices, but that information about which users are infected is not made available to others.

Furthermore, all the apps, to a greater or lesser degree, restrict the information that is exchanged between devices. The New Zealand app allows no information to be exchanged between devices, but encounters are inferred ex post based on shared attributes (i.e., locations and activities recorded by each user). Device-to-device transmissions are limited in the other four apps analysed: the only information exchanged are the user identifiers required to represent encounters (possibly contingent on further thresholds of data collection).

Finally, some measures exist within all the apps to ensure the accuracy and completeness of personal information. To enhance data integrity, the Australian, Japanese, and New Zealand apps require some type of initial verification to set up the app. The French, German, and Japanese apps require users to verify their test results when declaring themselves infected with Covid-19. To do so, they receive a one-time code that can be entered in multiple ways to prevent misreporting and ensure that information is entered reliably. Similarly, the New Zealand app provides multiple ways to enter locations and activities and to add supplementary information to encourage completeness. It also lets users review their digital profiles and revise and complement their visits and other information. Similarly, the Australian app allows users to reinstall the app to correct personal information. As a rule, however, all the apps—except for the one deployed in New Zealand—store encounter information in a secure section of the device that cannot be accessed by users; this prevents users from reidentifying other users, particularly infected persons.

5 Theoretical Evaluation of Information Privacy in the Context of Covid-19 Contact Tracing Apps

Thus far, we have analysed design principles evident from existing Covid-19 contact tracing apps, based on the broad understanding of information privacy as limited access to information about a person (*condition of privacy*) who might be able to control, to a certain extent, how that information is accessed and used (*management of privacy*). Table 5 summarises the normative and technical design principles to protect users' information privacy.

	Normative design principles to protect information privacy	**Technical design principles to protect information privacy**
Design principles aimed at limiting access to personal information (*condition of privacy*)	*Does not apply.*	- Data minimisation - Data protection (centralised vs. decentralised) - Pseudonymisation
Design principles aimed at granting users control over their personal information (*management of privacy*)	- Voluntariness - Transparency	- Data quality enhancement

Table 5 Normative and technical design principles to protect users' information privacy

Based on the findings of the exploratory analysis, we conclude that the understanding of limited access to personal information that is evident from the apps varies along two dimensions. The first is the *centralised-decentralised dimension*. The Australian and French apps in particular pursue a centralised approach, meaning that they do not transmit information about infected users to others' devices, but perform all matching and processing of personal information on central servers. In contrast, the decentralised approach of the German and

Japanese apps, and, somewhat differently, the New Zealand app, entrusts users' devices with these tasks, largely reducing central servers to a transmittal function.

The second dimension, which we refer to as the *data minimisation-richness dimensi*on, is based on the data minimisation and pseudonymisation design principles evident from our analyses. Along this dimension, the German, French, and Japanese apps limit access to personal information by minimising the information collected and through effective use of logically disconnected user pseudonyms to eliminate illegitimate access to person or user identifying information. In contrast, the Australian and the New Zealand apps specifically ask users to contribute personal information to be used for enhanced risk assessment and contact tracing.

With respect to the management of information privacy, the voluntariness and transparency principles relate to choice and consent; they enable users to control whether and what information about themselves they make available in the first place. *Voluntariness* implies that users can choose whether to use the apps and, if they do so, whether to provide the requested information. For instance, users who test positive for Covid-19 can decide whether to make that information available to others or can use the app without doing so and still receive warnings—although the effectiveness of contact tracing would clearly suffer. *Transparency* implies that users can make informed decisions about using the app based on the information provided.

In contrast, measures that allow for *enhancement of data quality* relate to the ex-post correction of personal information that has been collected. While this does not protect users from illegitimate access and use of their personal information, it does enable them to ensure that such information is accurate, complete, and up to data, and hence that adequate conclusions (in particular about their own and others' risk status) can be drawn. This tradeoff between design principles for limiting and managing access to personal information indicates that the former may come at the expense of generating more precise and targeted warnings.

The design principles for limiting access to users' personal information we identified are, in principle, technical, as they can—depending on the effectiveness of their implementation—reduce exposure to unwarranted access to and prevent accumulation and recombination of personal information. Such technical measures can only help constitute naturally private situations, where user personal information is protected from particular violations as a matter of fact, but implemented protections do not grant normative rights to information privacy. Similarly, design principles related to correction through data quality enhancement are inherently technical, as they provide actual opportunities for users to revise and complement personal information. In contrast, design principles for managing information privacy through choice and consent are primarily normative. While the documentation for all the apps state that voluntariness and transparency are desirable, they do not describe measures taken to ensure they are obeyed. For instance, it is beyond the scope of app design to ensure that health agencies and other agents do not take measures to enforce app use.

6 Discussion

Our insights into the normative and technical design principles are clearly related to the broader discourse in information systems and other disciplines regarding the adoption and use of mobile applications for contact tracing, and parallel the findings of prior research on information privacy in the context of Covid-19 contact tracing apps.

Our findings confirm that the design of apps deployed early on by five liberal democracies considers key ethical principles identified in the literature. In particular, the documentation we analysed stress the role of *voluntariness*, which is deemed crucial for privacy-sensitive design. The voluntariness principle goes beyond the mere adoption of an app, but includes people's decisions to carry a smartphone, download and install the app, leave the app operating in the background, react to alerts, share contact logs if they test positive, and uninstall the app together with removing collected data (Klar & Lanzerath, 2020).

However, voluntariness only protects people's information privacy in a normative sense. As Ishmaev et al. (2021) point out, even if adoption and use of apps for Covid-19 contact tracing is declared non-mandatory, social or economic conditions may still create pressure to do so. Voluntariness is also contingent on user understanding of how and what information is accessed by the apps. In an early analysis, Zhang, Chow, and Smith (2020) conclude that the privacy-related information provided by the Australian and New Zealand app documentation, for instance, may be too complex for users to read and understand. Also, only two of the apps have open source code, meaning that in-depth inspection of the apps' functionalities even by experts is not always possible, leaving the implementation of normative information-privacy protections to the responsible institutions' goodwill and competences.

What is more, proportionality is a key criterion for privacy-sensitive app design (Morley et al., 2020). However, concerns were raised that contact tracing apps may not be effective in containing the spread of Covid-19 because they can make a real difference only if a significant percentage of the population (e.g., 56% or more) use them (Hinch et al., 2020). If that threshold is not met—as was the case in the five countries at the time of our study—a potential sacrifice of information privacy may be unjustified.

Overall, many privacy-related aspects—in particular, voluntariness, user consent, anonymity (in terms of pseudonymisation), purpose specification, provision of app providers' contact information, and specification of data retention parameters and the decommissioning process (Klar & Lanzerath, 2020; Morley et al., 2020)—have been systematically addressed by the apps analysed. However, not all have adopted corresponding design principles in equal measure, and other potential threats to user information privacy, such as special protection of data collected from children, updates to the apps' privacy policy changes, and privacy breach notices (e.g., Hatamian et al., 2021; Kolasa, Mazzi, Leszczuk-Czubkowska, Zrubka, & Péntek, 2021), are not explicitly evident from the apps' accompanying documentation. While we expect that such issues have been addressed since our study was completed, it is revealing how even proactive privacy-sensitive app design may deviate at least from some of the previously suggested ethical standards.

In addition, works such as that of Hatamian et al. (2021) suggest that the extent to which the applied design principles are actually suited to limit access to personal information depends considerably on their actual implementation—which, according to them, still leaves room for improvement. In addition, further measures that could be taken, such as data protection through random noise signals (e.g., Sharma & Bashir, 2020), have not (yet) been explicitly addressed by the majority of apps we have analysed.

Our findings hint at an unsurprising but nevertheless critical tension between normative and technical design principles: if normative principles, such as voluntariness and transparency, are not supported by technical measures, the risk of information privacy violations could be

real. If, for instance, information-privacy policy documentation is insufficient, or people are encouraged to use the app to avoid other constraints, these principles could be undermined. However, if technical protections such as secure storage and pseudonymisation lack normative justification, they can only be evaluated against the benchmark of the efficacy of implementation—which is not feasible for laypersons, and which may undergo unnoticed changes at any time.

Contrasting the design principles identified from the apps analysed, we find striking similarities between the information-privacy standards they set. This is likely due to the homogeneous sample of apps originating from liberal democracies. It is hence not unexpected that these apps afford similar levels of information privacy. Still, from a theoretical point of view, it is interesting to see what the apps' design reveals about the understanding of information privacy. One aspect in this regard is the distinction between centralised and decentralised storage. Both approaches can, in principle, be privacy preserving (WHO, 2020); still, they are based on different assumptions regarding the origins of potential information privacy threats. While centralised design stresses the risk that individual users might recombine distinct pieces of information about others and thus re-identify other users and draw conclusions about their health status, decentralised design emphasises threats due to the existence of central stores of aggregated information that, if compromised, could expose a large number of users.

Another aspect relevant for our theoretical understanding of information privacy is the tension between data minimisation and pseudonymisation, on the one hand, and the data richness demand posed by several apps, on the other. The former stresses the condition of privacy, where access to personal information is largely restricted. It is in line with the postulate to favor privacy by default to ensure exposure to potential information-privacy violations is effectively minimised, and it is clearly in line with much prior research that interprets information privacy in terms of autonomy, or the absence of intrusion into users' private sphere (Becker, 2019).

While all the apps analysed generally agree that certain types of personal information, such as GPS data, is not necessary to enable contact tracing and hence should not be collected (WHO, 2021a), the data richness postulate indicates a more differentiated view regarding what constitutes illegitimate access to and use of user personal information, such that particular types of personal information (e.g., health status information) demand higher levels of protection than others that may be shared more carelessly. It hence shifts the focus of information privacy from autonomy to integrity, ensuring appropriate representation of users through their personal information based on a notion of information privacy as effective control over the flow of such information in a given context (as postulated by, for instance, Floridi, 2006).

7 Conclusion

In summary, we have analysed the normative and technical design principles through which Covid-19 contact tracing apps deployed in five liberal democracies aspire to protect information privacy: voluntariness, transparency, data minimisation, pseudonymisation, protection of personal information (through centralised and decentralised designs), and data quality enhancement.

The contributions of disclosive computer ethics studies can be found at three levels: the *disclosure level*, which explicates the hidden moral properties of the technological artifacts under study; the *theoretical level*, which refines and further develops existing theory; and the *application level*, which refers the theoretical insights back to the disclosure level (Brey, 2000a, 2000b). At the disclosure level, in response to RQ1, we have spelled out the normative and technical design principles through which the apps analysed protect information privacy. At the theoretical level, in response to RQ2, we have explained what these principles reveal about the understanding of information privacy that has, explicitly or implicitly, guided the design of these apps, and how this relates to the condition and management of information privacy according to the RALC framework. Furthermore, we have discussed how the principles identified complement or contradict each other, and how these evident tensions can enrich our theoretical understanding of information privacy in the given context. Finally, at the application level, we expect that our insights can inform the design of contact tracing apps and help evaluate the measures taken to protect user information privacy both in newly released apps and in updated versions of the apps analysed.

The contribution of our work lies in the space between normative papers that develop design guidelines from an ethical perspective (e.g., Morley et al., 2020) and technical papers that analyse how those guidelines are implemented (e.g., Hatamian et al., 2021). Our work is intended to inform app design by providing real-world examples of privacy-sensitive design that are motivated by well-grounded ethical theory and inspired by practical examples. Thus, we approach the refinement of ethical theory to develop and evaluate design principles for actually usable technological artifacts, as demanded, amongst others, by Bélanger and Crossler (2011).

Our argument is based on the RALC framework of information privacy (Moor, 1997; Tavani & Moor, 2001), which conceptualises information privacy in terms similar to much information systems research: as a state in which access to information about a person is limited, or in which people are able to control information about themselves (Popovič, Smith, Thong, & Wattal, 2017; Smith et al., 2011). It captures the potential of technological artifacts to threaten information privacy while also providing opportunities for users manage it actively, and is said to be sufficiently comprehensive to apply to a wide range of related concerns (Tavani, 2007).

As Solove (2006) explains, privacy theories will typically have problems to apply to information privacy in digital environments, as the corresponding information and communications technologies have capacities to collect, store, process, and disseminate information about their users that go well beyond those of the means of communication addressed in the original debates. In addition, few existing theories recognise privacy breaches that result from practices such as the constant and unobtrusive surveillance of users, data mining, and user profiling, which are nonetheless key information privacy concerns put forth in the given context (Clarke, 2019; Stahl, 2019; Volokh, 2000). Still, our theoretical perspective implies that the interpretations put forth in this paper are meaningful only in the context of the RALC framework, which, as we have discussed, may have issues accounting for the trade-off between users' autonomy and the integrity of representation.

Another limitation comes from the small sample of apps we analysed. Our results are based on apps deployed as early as June 2020 in liberal democracies, which means that our contribution is restricted to outlining example design principles rather than providing a

representative summary. Further, different countries will typically continue to pursue different approaches to the development of apps, owing to social and cultural preferences and path dependencies. To raise awareness of alternative approaches and justifications, we have articulated what we think are the evident design choices. Our results are by no means final, as apps are typically developed further while in use, and new contact tracing apps have become available since we conducted our study. What is more, while official documentation is an informative source of information, complementary analyses would be required to determine, for instance, the effectiveness of how the principles we identified were implemented.

Our work is also relevant for the design of digital information and communications technologies in other social and economic settings with the potential for large-scale data collection and public surveillance, which are on the rise. For instance, fitness apps enable the large-scale collection of fitness and health data: where, when, and for how long users are active and with whom they compare themselves. Widely used dating apps enable matches between users based on their geographical locations and other criteria. Restaurants and hotels use apps and similar tools to manage reservations digitally, saving customer data that is often poorly protected in cloud services with little regard for or even awareness of information privacy issues (Chaos Computer Club, 2020). For those, knowledge of existing conceptualisations of information privacy and corresponding design principles could be particularly useful.

Information privacy is of growing interest in information systems research, as the digitisation of different sorts of information increases, along with the use of technology and methods for capturing information, such as online platforms and big data analysis. We responded to calls for more context-specific research in this area: that digital artifacts and privacy-related practices need to be analysed within the context they are used; and that theories from other fields need to be applied meaningfully given that information security is an interdisciplinary research field (e.g., Bélanger & Crossler, 2011; Lowry, Dinev, & Willison, 2017). We focused on disclosing and integrating moral properties evident from existing technological artifacts, and so the outcome of our work cannot be characterised as full-fledged ethical theory. Rather, we have illustrated how ethical theory can inform the design of technological artifacts in general, and how empirical design choices can contribute to advancing such theory vice versa.

In ethical terms, privacy theory must include not only a descriptive account of but also a normative justification of privacy (Parent, 1983). In this paper, we have clearly focused on the former. A normative justification that clarifies not only whether information privacy is present in a certain artifact, but also the extent to which there is a justifiable claim to information privacy in a certain use context, would be valuable, especially for Covid-19 tracing apps. With respect to Covid-19, there are alternative approaches (e.g., tracking apps) that are generally regarded as less privacy friendly than the tracing apps we have analysed, and by far not all countries deploy those apps on a voluntary basis for people to use at their own discretion. Our work should hence be seen as an initial step towards challenging and refining existing ethical theory.

References

Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., Jha, S. K. (2020). A Survey of COVID-19 Contact Tracing Apps. *IEEE Access*, *8*, 134577–134601. https://doi.org/10.1109/ACCESS.2020.3010226

Australian Government (2020). Privacy Policy. Retrieved from https://covidsafe.gov.au/privacy-policy.html*, accessed on 11th July 2020.

Australian Government Department of Health (2020). COVIDSafe App. Retrieved from https://www.health.gov.au/resources/apps-and-tools/covidsafe-app#get-th*, accessed on 11th July 2020.

Becker, M. (2019). Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy. *Ethics and Information Technology*, *21*(4), 307–317. https://doi.org/10.1007/s10676-019-09508-z

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MISQuarterly*, *35*(4), 1017–1041.

Blasimme, A., & Vayena, E. (2020). What's next for COVID-19 apps? Governance and oversight. *Science (New York, N.Y.)*, *370*(6518), 760–762. https://doi.org/10.1126/science.abd9006

Boutet, A., Bielova, N., Castelluccia, C., Cunche, M.: Lauradoux, C., Le Métayer, D., & Roca, V. (2020). Proximity Tracing Approaches - Comparative Impact Analysis. Retrieved from https://hal.inria.fr/hal-02570676v1*, accessed on 20th August 2020.

Brey, P. (2000a). Disclosive Computer Ethics. *ACM SIGCAS Computers and Society*, *30*(4), 10–16. https://doi.org/10.1145/572260.572264

Brey, P. (2000b). Method in Computer Ethics: Towards a Multi-Level Interdisciplinary Approach. *Ethics and Information Technology*, *2*(2), 125–129. https://doi.org/10.1023/A:1010076000182

Budd, J., Miller, B. S., Manning, E. M., Lampos, V., Zhuang, M., Edelstein, M., . . . McKendry, R. A. (2020). Digital technologies in the public-health response to COVID-19. *Nature Medicine*, *26*(8), 1183–1192. https://doi.org/10.1038/s41591-020-1011-4

Campbell, J. E., & Carlson, M. (2002). Panopticon.com: Online Surveillance and the Commodification of Privacy. *Journal of Broadcasting & Electronic Media*, *46*(4), 586–606. https://doi.org/10.1207/s15506878jobem4604_6

Chan, E. Y., & Saqib, N. U. (2021). Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior*, *119*, 106718. https://doi.org/10.1016/j.chb.2021.106718

Chaos Computer Club (2020). CCC hackt digitale "Corona-Listen". Retrieved from https://www.ccc.de/de/updates/2020/digitale-corona-listen/*, accessed on 29th August 2020.

Clarke, R. (1999). Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM*, *42*(2), 60–67. https://doi.org/10.1145/293411.293475

Clarke, R. (2019). Risks Inherent in the Digital Surveillance Economy: A Research Agenda. *Journal of Information Technology*, *34*(1), 59–80. https://doi.org/10.1177/0268396218815559

Corona Warn App Open Source Project (2020). Frequently Asked Questions about the Corona-Warn-App. Retrieved from https://www.coronawarn.app/en/faq/*, accessed on 29th June 2020.

Di Gennaro, F., Pizzol, D., Marotta, C., Antunes, M., Racalbuto, V., Veronese, N., & Smith, L. (2020). Coronavirus Diseases (COVID-19) Current Status and Future Perspectives: A Narrative Review. *International Journal of Environmental Research and Public Health*, *17*(8). https://doi.org/10.3390/ijerph17082690

European Commission (2020). COMMUNICATION FROM THE COMMISSION: Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data. Retrieved from https://ec.europa.eu/info/sites/default/files/5_en_act_part1_v3.pdf*, accessed on.

European Parliament (2020). Covid-19 tracing apps: ensuring privacy and use across borders, accessed on November 5, 2020.

The Federal Government (2020a). The Corona-Warn-App: Helps us Fight the Coronavirus. Retrieved from https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-englisch*, accessed on 29th June 2020.

The Federal Government (2020b). Frequently Asked Questions. Retrieved from https://www.bundesregierung.de/breg-de/themen/corona-warn-app/corona-warn-app-englisch/corona-warn-app-faq-1758636*, accessed on 29th June 2020.

Fischer, D., Hattori-Putzke, J., & Fischbach, K. (2019). Crisis Warning Apps: Investigating the Factors Influencing Usage and Compliance with Recommendations for Action. In *Proceedings of the Hawai'i International Conference on System Science*.

Floridi, L. (2006). Four Challenges for a Theory of Informational Privacy. *Ethics and Information Technology*, *8*(3), 109–119. https://doi.org/10.1007/s10676-006-9121-3

Floridi, L. (2020). Mind the App-Considerations on the Ethical Risks of COVID-19 Apps. *Philosophy & Technology*, 1–6. https://doi.org/10.1007/s13347-020-00408-5

Fodor, M., & Brem, A. (2015). Do privacy concerns matter for Millennials? Results from an empirical analysis of Location-Based Services adoption in Germany. *Computers in Human Behavior*, *53*(2), 344–353. https://doi.org/10.1016/j.chb.2015.06.048

Hatamian, M., Wairimu, S., Momen, N., & Fritsch, L. (2021). A privacy and security analysis of early-deployed COVID-19 contact tracing Android apps. *Empirical Software Engineering*, *26*(3), 36. https://doi.org/10.1007/s10664-020-09934-4

Inria (2020a). FAQ on the Technical Aspects of the StopCovid Application. Retrieved from https://www.inria.fr/en/faq-technical-aspects-stopcovid-application*, accessed on 3rd July 2020.

Inria (2020b). StopCovid Inria Press Release. Retrieved from https://www.inria.fr/en/stopcovid*, accessed on 3rd August 2020.

Inria (2020c). The StopCovid Project-Team Starts Publishing the Source Code and Documentation of the StopCovid Application. Retrieved from https://www.inria.fr/en/stopcovid-source-code*, accessed on 3rd August 2020.

Ishmaev, G., Dennis, M., & van den Hoven, M. J. (2021). Ethics in the COVID-19 pandemic: Myths, false dilemmas, and moral overload. *Ethics and Information Technology*, 1–16. https://doi.org/10.1007/s10676-020-09568-6

Klar, R., & Lanzerath, D. (2020). The Ethics of COVID-19 Tracking Apps – Challenges and Voluntariness. *Research Ethics*, 1-9. https://doi.org/10.1177/1747016120943622

Kolasa, K., Mazzi, F., Leszczuk-Czubkowska, E., Zrubka, Z., & Péntek, M. (2021). State of the Art in Adoption of Contact Tracing Apps and Recommendations Regarding Privacy Protection and Public Health: Systematic Review. *JMIR MHealth and UHealth*, *9*(6), e23250. https://doi.org/10.2196/23250

Lowry, P. B., Dinev, T. [Tamara], & Willison, R. (2017). Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research agenda. *European Journal of Information Systems*, *26*(6), 546–563. https://doi.org/10.1057/s41303-017-0066-x

Ministére De L'économie des Finances et de la Relance (2020a). FAQ StopCovid. Retrieved from https://www.economie.gouv.fr/stopcovid-faq*, accessed on 3rd July 2020.

Ministére De L'économie des Finances et de la Relance (2020b). https://www.economie.gouv.fr/stopcovid. Retrieved from https://
www.economie.gouv.fr/stopcovid#*, accessed on 3rd July 2020.

Ministry of Health (2020a). NZ COVID Tracer App. Retrieved from https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-novel-coronavirus-resources-and-tools/nz-covid-tracer-app*, accessed on 31st July 2020.

Ministry of Health (2020b). Questions and Answers on NZ COVID Tracer. Retrieved from https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-novel-coronavirus-resources-and-tools/nz-covid-tracer-app/questions-and-answers-nz-covid-tracer*, accessed on 31st July 2020.

Ministry of Health, Labour and Welfare (2020a). Contact Confirmation Application Privacy Policy. Retrieved from https://www.mhlw.go.jp/stf/seisakunitsuite/english_pp_00032.html*, accessed on 31st July 2020.

Ministry of Health, Labour and Welfare (2020b). Q & A for Users of the Contact Tracing App. Retrieved from https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/covid19_qa_kanrenkigyou_00009.html*, accessed on 31st July 2020.

Moor, J. H. (1997). Towards a Theory of Privacy in the Information Age. *ACM SIGCAS Computers and Society*, *27*(3), 27–32. https://doi.org/10.1145/270858.270866

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

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, *17*(5/6), 559. https://doi.org/10.2307/3505189

Pan, A., Liu, L., Wang, C., Guo, H., Hao, X., Wang, Q., . . . Wu, T. (2020). Association of Public Health Interventions With the Epidemiology of the COVID-19 Outbreak in Wuhan, China. *JAMA*, *323*(19), 1915–1923. https://doi.org/10.1001/jama.2020.6130

Parent, W. A. (1983). Privacy, Morality, and the Law. *Philosophy & Public Affairs*, *12*(4), 269–288. Retrieved from http://www.jstor.org/stable/2265374

Popovič, A., Smith, H. J., Thong, J. Y. L., & Wattal, S. (2017). MIS Quarterly Research Curation on Information Privacy. *MIS Quarterly*, *Updated: June 2018; August 2019*.

Repucci, S., & O'Toole, S. (2020). *Freedom in the World 2020: The Annual Survey of Political Rights & Civil Liberties*. New York, NY, Washington, DC and Lanham, Boulder, New York, London: Freedom House and Rowman & Littlefield.

Rowe, F. (2020). Contact Tracing Apps and Values Dilemmas: A Privacy Paradox in a Neo-Liberal World. *International Journal of Information Management*, 102178. https://doi.org/10.1016/j.ijinfomgt.2020.102178

Sharma, T., & Bashir, M. (2020). Use of apps in the COVID-19 response and the loss of privacy protection. *Nature Medicine*, *26*(8), 1165–1167. https://doi.org/10.1038/s41591-020-0928-y

Smith, H. J., Dinev, T. [T.], & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989. https://doi.org/10.2307/41409970

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477. https://doi.org/10.2307/40041279

Stahl, B. C. (2019). Teaching Ethical Reflexivity in Information Systems: How to Equip Students to Deal With Moral and Ethical Issues of Emerging Information and Communication Technologies. *Ournal of Information Systems Education*, *22*(3), 253–260.

Stahl, B. C. (2012). Morality, Ethics, and Reflection: A Categorization of Normative IS Research. *Journal of the Association for Information Systems*, *13*(8), 636–656. https://doi.org/10.17705/1jais.00304

Taddeo, M. (2020). The Ethical Governance of the Digital During and After the COVID-19 Pandemic. *Minds and Machines*, 1–6. https://doi.org/10.1007/s11023-020-09528-5

Tavani, H. T. (2007). Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy. *Metaphilosophy*, *38*(1), 1–22. https://doi.org/10.1111/j.1467-9973.2006.00474.x

Tavani, H. T. (2008). Informational Privacy: Concepts, Theories, and Controversies. In K. E. Himma & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 131–164). Hoboken, N.J: Wiley. https://doi.org/10.1002/9780470281819.ch6

Tavani, H. T., & Moor, J. H. (2001). Privacy Protection, Control of Information, and Privacy-Enhancing Technologies. *ACM SIGCAS Computers and Society*, *31*(1), 6–11. https://doi.org/10.1145/572277.572278

Trang, S., Trenz, M., Weiger, W. H., Tarafdar, M., & Cheung, C. M.K. (2020). One App to Trace Them All? Examining App Specifications for Mass Acceptance of Contact-Tracing Apps. *European Journal of Information Systems*, *94*(1), 1–14. https://doi.org/10.1080/0960085X.2020.1784046

Volokh, E. (2000). Personalization and Privacy. *Communications of the ACM*, *43*(8), 84–88. https://doi.org/10.1145/345124.345155

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

WHO (2021a). Contact tracing in the context of COVID-19. Retrieved from https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19*, accessed on.

WHO (2021b). COVID-19 Strategic Preparedness and Response Plan (SPRP 2021). Retrieved from https://www.who.int/publications/i/item/WHO-WHE-2021.02*, accessed on November 27th, 2021.

Woodhams, S. (2020). COVID-19 Digital Rights Tracker. Retrieved from https://www.top10vpn.com/research/covid-19-digital-rights-tracker/*, accessed on November 5, 2021.

Zastrow, M. (2021). Coronavirus contact-tracing apps: can they slow the spread of COVID-19? Retrieved from https://www.nature.com/articles/d41586-020-01514-2*, accessed on October 26, 2021.

Zhang, M., Chow, A., & Smith, H. [Helen] (2020). Covid-19 Contact-Tracing Apps: Analysis of the Readability of Privacy Policies. *Journal of Medical Internet Research*, *22*(12), e21572. https://doi.org/10.2196/21572

doi: https://doi.org/10.3127/ajis.v26i0.3097