



UvA-DARE (Digital Academic Repository)

Exploring people's perceptions and support of data-driven technology in times of COVID-19: the role of trust, risk, and privacy concerns

Zarouali, B.; Strycharz, J.; Helberger, N.; de Vreese, C.

DOI

[10.1080/0144929X.2021.2022208](https://doi.org/10.1080/0144929X.2021.2022208)

Publication date

2022

Document Version

Final published version

Published in

Behaviour and Information Technology

License

CC BY-NC-ND

[Link to publication](#)

Citation for published version (APA):

Zarouali, B., Strycharz, J., Helberger, N., & de Vreese, C. (2022). Exploring people's perceptions and support of data-driven technology in times of COVID-19: the role of trust, risk, and privacy concerns. *Behaviour and Information Technology*, 41(10), 2049-2060. <https://doi.org/10.1080/0144929X.2021.2022208>

General rights


It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (<https://dare.uva.nl>)

Exploring people's perceptions and support of data-driven technology in times of COVID-19: the role of trust, risk, and privacy concerns

Brahim Zarouali ^a, Joanna Strycharz^a, Natali Helberger^b and Claes de Vreese ^a

^aAmsterdam School of Communication Research (ASCoR), University of Amsterdam, Amsterdam, The Netherlands; ^bInstitute for Information Law (IViR), University of Amsterdam, Amsterdam, The Netherlands

ABSTRACT

The COVID-19 pandemic has created one of the largest medical, financial, and social disruption in history. In the fight against this virus, many European governments have turned to collecting and using online data (for various technological applications) as a key strategic remedy. This study consists of data from a national representative survey in the Netherlands focusing on the extent to which data-driven technologies from the government can count on the support of the general public. By focusing on trust perceptions, risk beliefs and privacy concerns, we introduce a typology consisting of three subgroups: the *sceptical*, the *carefree*, and the *neutral* respondents. It was found that each of the three groups exhibit unique demographic characteristics. In addition, findings also revealed that these three identified groups have different support levels for specific digital solutions from the government. These findings contribute to an important and timely debate and entail relevant policy implications with regard to the democratic legitimization of data-driven technologies in times of COVID-19.

ARTICLE HISTORY

Received 3 March 2021
Accepted 18 December 2021

KEYWORDS

COVID-19; data-driven technologies; government; trust; risk; privacy

1. Introduction

In the beginning of 2020, the world witnessed how the outbreak of a novel coronavirus (COVID-19) rapidly resulted in countries shutting down their borders and issuing very severe quarantines. In tackling the unprecedented challenges of this global pandemic, digital technology can play a pivotal role (UN 2020). Many European governments swiftly announced the possible collection and use of people's personal data in the fight against the COVID-19 virus. Indeed, governments have started to collaborate with private companies, such as mobile network operators, location intelligence companies and AI technology companies to enrol data-driven tools in the fight against COVID-19 (Budd et al. 2020; UN 2020; Whitelaw et al. 2020). For a successful implementation of these digital tools, access to personal data (of citizens) is critical. However, much is yet to be explored about what people think of these digital solutions that exploit their data. As argued by the World Health Organisation, the effectiveness of such data-driven solutions largely depends on the levels of trust and support that a given population has in their own government to securely enrol this digital agenda (WHO 2020).

In addition, because the deployment of those technological measures typically comes along with what McDonald (2020) describes as 'seizure of power', and in so doing may affect individual rights (such as privacy and data protection), they require democratic legitimisation (Craglia et al. 2020). From the perspective of democratic legitimisation, it is important to investigate to what extent governmental data collection can count on the support of the people that will be affected by it (while focusing on whether certain parts of the population stand more behind this practice), as well as explore to what extent they support specific technological measures as worthwhile solutions in the global pandemic.

In this study, a survey was distributed among a national representative sample of $N = 907$ respondents in the Netherlands. The aims were twofold. First, we wanted to explore people's trust, risk and privacy concerns toward their data being collected by the government in the fight against COVID-19. The study draws on the tenets of *social contract theory* (Dunfee, Smith, and Ross 1999). Based on this framework, a first research question was formulated: *which different groups of individuals can be distinguished based on trust perceptions, risk beliefs, and privacy concerns (in*

CONTACT Brahim Zarouali  b.zarouali@uva.nl  Amsterdam School of Communication Research (ASCoR), University of Amsterdam, NieuweAchtergracht 166, 1018 WV Amsterdam, The Netherlands

© 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

the context of collecting and using personal data in the fight against COVID-19? To answer this question, we used a cluster analysis (K-means) because it provides an effective and meaningful approach to classify the sampled individuals in our exploratory dataset into homogeneous groups and allows for a deeper understanding of these groups as well. In total, three groups were identified (i.e. the sceptical, the carefree and the neutral respondents), and their demographic characteristics and differences are discussed in more detail. The second research question of this paper is to further explore whether these subgroups have different levels of 'support' for specific digital measures in the combat against COVID-19. This resulted in a second research question: *what are the differences between the subgroups in terms of support toward specific digital solutions of the government in the fight against COVID-19?* We investigate people's support toward a broad range of solutions including proximity tracing, hospital management, vaccine development, public communication, quarantine compliance, and disinformation detection (Budd et al. 2020; Gasser et al. 2020; UN 2020). We examine whether and to what extent the three subgroups which are identified (sceptics, carefree, and neutral) differ from each other when it comes to supporting these digital measures in the fight against COVID-19.

This paper makes multiple contributions. First, it examines how people differ in their perceptions toward the social contract in the context of governmental data collection. Measuring three constructs central to social contract in this context, we can identify underlying clusters among citizens that reflect the versatility of the theory. Second, once these groups are identified, we can assess why some individuals accept different digital solutions used in the fight against COVID-19 and others do not. This carries substantial practical implications as insights into support of digital solutions among different societal groups are crucial for democratic legitimisation of digital measures taken by the government during a global pandemic.

2. Theoretical framework

2.1. The importance of trust, risk and privacy concerns

In 2020, the COVID-19 pandemic has spread like wildfire across the whole world. In the early days of the pandemic, many governments announced to use technologies to help contain its spread. Many of these data-driven solutions come with wide-ranging implications for people's privacy, which has fuelled much concerns among civil society actors (French and Monahan 2020; Lewandowsky

et al. 2021). From the perspective of democratic legitimacy, it is important to explore what extent governmental data collection (for the purpose of rolling out digital technologies) can count on the support or acceptance by the general population. To answer the question of public acceptance of digital solutions, prior research has often focused on three important factors: people's *trust beliefs*, *risk perceptions*, and *privacy concerns* (Kalliopi 2016; Tang, Hu, and Smith 2008).

When it comes to trust, it is the result of a trustor's evaluation of how likely the trustee will behave according to the trustor's expectations (Baier 1986; Bauer 2014; Coleman 1990). In the context of this study, trust beliefs refer to degree to which people believe the government is trustworthy in protecting their personal data (Malhotra, Kim, and Agarwal 2004). It is important that citizens believe that their government is generally acting in their best interest and perceive their government to be capable of collecting and managing their personal data in a safe, secure and transparent way. Recent studies on technological solutions during COVID-19 (e.g. contact tracing apps) showed that trust in the government influences peoples' response and perception toward that technological solution (Altmann et al. 2020; Moon 2020; Oldeweme et al. 2021).

Risk perception refers to people's perceptions of the uncertainty and adverse consequences of handing over their data to the government (Dowling and Staelin 1994). Scholars have argued that perceived risk might be an important factor in determining citizens' acceptance and adoption of online services from the government (Bélanger and Carter 2008; Warkentin et al. 2002), and that these perceptions can be an important barrier for accepting data collection by the government (Beldad, de Jong, and Stehouder 2011). In the context of Covid-19, it has been found that risk perceptions related to data security can influence the acceptance of digital solutions installed by the government, such as tracing apps (e.g. Albrecht et al. 2021).

Privacy concern refers to the degree to which a user is concerned about threats to their informational privacy online, usually in the context in which their personal data is being collected (Xu, Michael, and Chen 2013). Data privacy has always been a very important factor influencing citizens' acceptance of governmental surveillance and monitoring (e.g. Nam 2019; Pavone and Esposti 2012; Thompson et al. 2008). In times of COVID-19, privacy concerns have been consistently found to be an important impediment in accepting and adopting technological solutions from the government (e.g. Abuhammad, Khabour, and Alzoubi 2020; Altmann et al. 2020; Chan and Saqib 2021; Kosterink et al. 2020). It is therefore one of the main

considerations to acknowledge in the technology-driven COVID-19 response (Redmiles 2021).

To connect these three concepts in a theoretical way, we will draw on the tenets of *social contract theory* in the next section.

2.2. Social contract theory

To explore people's perceptions of the government collecting and monitoring personal data in the fight against the COVID-19 disease, we employ social contract theory (Dunfee, Smith, and Ross 1999). This theory has often been used as a meaningful conceptual framework to investigate people's perceptions about data collection and informational privacy (e.g. Culnan and Bies 2003; Fogel and Nehmad 2009; Kruikeimeier, Boerman, and Bol 2020; Malhotra, Kim, and Agarwal 2004; Martin 2016). As an important theory in political philosophy, it is relevant in explaining the legitimisation of governments to collect and process personal data of citizens (Economides 2018). Recent studies also highlighted the usefulness of a social contract perspective in times of COVID-19 (e.g. Ramelet 2020; Razavi et al. 1999; Voigt 2021), because the pandemic brings the implicit social contract between every citizen and their government to centre stage (Zivin and Sanders 2020). According to a social contract, all citizens are bound to do their share for the community by obeying the laws, rules and measures installed by the government during a pandemic; and in exchange, they benefit from the public goods provided by the government (e.g. safety, health, etc.), which are dependent upon citizen's compliance with the rules and measures (Ramelet 2020).

In the context of the adoption of data-driven digital solutions, such a social contract could be understood as a 'mutual agreement' between individuals and the government about how their data is used and shared (Martin 2012, 2016) with the goal of managing the COVID-19 crisis. This means that individuals share their personal information with the government and trust that this institution handles their data safely because the government has the moral and legal obligation to protect it (i.e. the implied social contract) (Kruikeimeier, Boerman, and Bol 2020; Okazaki, Li, and Hirose 2010). However, not every individual is willing to share personal data with the government as not everyone may *perceive* the social contract to be equally reliable and/or desirable (Martin 2016, 2012). Following this line of reasoning, an important question is: what are the 'perceptions' that people take into account in evaluating the implied social contract with the government? A recent study by Kruikeimeier, Boerman, and Bol

(2020) found that the three variables discussed in the previous section, i.e. trust beliefs, risk perceptions, and privacy concerns, play a pivotal role in a mutual social contract.

When it comes to trust and risk perceptions, it has been asserted that they provide important foundations for a social contract (Okazaki, Li, and Hirose 2010). A vast amount of research shows that these two variables, trust and risk, are most salient in social contract theory in the context of information sharing (e.g. Culnan and Bies 2003; Fogel and Nehmad 2009; Okazaki, Li, and Hirose 2010). More specifically, when individuals trust the government to handle their data safely, the individual perceives the social contract as more reliable; but when individuals see a high-level risk associated with the handling of their data by the government, the implied social contract becomes less reliable. In addition to these two variables, it was found that *privacy concerns* are inextricably linked to the implied social contract as well (Bansal, Zahedi, and Gefen 2010; Fogel and Nehmad 2009; Sheehan 2002). When people have the perception that their (informational) privacy is not respected and their data not kept safe, they can perceive social contract with the government as less reliable, while low privacy concerns are related to high reliability of social contract.

Taken together, Kruikeimeier, Boerman, and Bol (2020) found that these three variables (i.e. privacy concerns, risk beliefs and trust perceptions) form the basis of a social contract; and that they can be used to cluster people in meaningful subgroups that are homogeneous with respect to these unobservable variables of interest. Following this evidence, we believe that these three variables (i.e. trust beliefs, risk perception and privacy concerns) would also be suitable to explore people's perceptions with regards to the government's intention to collect and use personal data to combat COVID-19. More precisely, we aim to investigate whether different *subgroups of people* can be identified based on these variables. In addition, we also aim to get a more fine-grained picture of these subgroups by exploring the similarities and differences between these clusters in terms of demographic composition. This allows to examine the prevalence and distribution of these subgroups among specific demographic cohorts. We propose the following exploratory research questions:

- RQ1: (a) In the context of collecting and using personal data in the fight against COVID-19, which different groups of individuals can be distinguished based on trust perceptions, risk beliefs, and privacy concerns (b) what are the main demographic characteristics of the people in these subgroups?

2.3. Supporting data-driven technological measures

Having discussed people's perceptions about the practice of governmental data collection, we will now zoom into how these data can be put to use to unlock the potential of technology in fighting the global pandemic (Whitelaw et al. 2020). That is, the reason why governments decide to collect and use data originating from a variety of digital sources is because it is a fundamental prerequisite for rolling out technological applications (Craglia et al. 2020). The use of such digital technologies has been presented as a key strategic remedy by governments in response to the COVID-19 pandemic. As argued by Gasser et al. (2020), technologies can be used to promptly alert and isolate exposed individuals (hereby preventing new infections), optimise public communication, increase the efficiency of healthcare, develop a vaccine, and improve quarantine measures.

This argument is entirely in line with recent reviews (e.g. Budd et al. 2020; Council of Europe 1990; Whitelaw et al. 2020), where some important areas were highlighted in which digital solutions can be harnessed: *proximity tracing* (i.e. using tracking technology to monitor individuals and inform them if they have been in contact with an infected patient), *digital (public) communication* (i.e. using digital communication platforms to quickly and efficiently inform the public), *hospital management* (using real-time data-driven methods to monitor the status of healthcare facilities, allocate health care resources, and increase hospital capacity), *vaccine development* (using recent advances in biotechnology and digital technologies to facilitate drug and vaccine development), and *quarantine compliance*

(using digital technology to monitor whether people comply with quarantine and self-isolation measures) are important areas in which digital solutions can be harnessed.

In addition to these four digital solutions, the EU Science Hub (i.e. the European Commission's science and knowledge service) also stressed the importance of an additional technological measure, i.e. using text mining algorithms and AI technology to automatically detect *onlined disinformation* about COVID-19 (European Commission 2020). The common denominator of these digital solutions is that they all use some kind of data about citizens (e.g. location data, patient health data, social media data, etc.). The effectiveness of these data-driven solutions is highly contingent on the support that citizens' may vest in these solutions (WHO 2020). Therefore, this study aims to investigate the support among the population for the abovementioned six digital solutions.

As part of the implied social contract that we discussed earlier, several studies found that people's privacy concerns, risk and trust perceptions (see RQ1) are foundational concepts that relate to how they respond to practices where their personal data is being collected online (Fogel and Nehmad 2009; Kruikemeier, Boerman, and Bol 2020). In other words, these three concepts might be critical in determining people's support level toward specific technological measures taken by their government. Following this line of reasoning, this study aims to explore to what extent the distinct subgroups from RQ1 (groups that are clustered based on their privacy concern, risk perceptions and trust beliefs) differ in terms of their support for the six digital solutions addressed above (i.e. digital communication, hospital management, vaccine development, quarantine, and disinformation) by the government in the combat against the coronavirus. Therefore, we propose this final research question:

RQ2: What are the differences between the subgroups (identified in RQ1) in terms of support toward specific digital solutions of the government in the fight against COVID-19?

Table 1. Socio-demographic characteristics of the sample.

	Percentage (%)	Frequency (N)
Age categories ($M_{\text{age}} = 50.87$, $SD_{\text{age}} = 15.90$)		
18–34 years	20.29	184
35–54 years	39.91	362
55+years	39.80	361
Gender		
Female	46.09	418
Male	53.91	489
Education		
Low	25.69	233
Moderate	50.39	457
High		
Region		
North	10.69	97
East	21.39	194
South	25.69	233
West	27.56	250
Three cities (Amsterdam, Rotterdam, and The Hague)	14.66	133

3. Methodology

3.1. Sample

The data consisted of a sample of $N = 907$ respondents in the Netherlands. This study was part of a larger survey focused on the impact of personalised communication and algorithms on society, which took on average 25 min to fill out. The response rate was 70%. The online survey ran from April 9 to April 20, 2020

(11 days during the COVID-19 ‘lockdown’ period) and was distributed by IPSOS, a global market research firm. Stratification based on age, gender and level of education was applied to make the sample comparable to the general population. The participants had a mean age of 50.87 ($SD = 15.90$ years), and 46% of them were women. Around 26% had a low (no education or primary education), 50% moderate (secondary education), and 24% higher education level (bachelor, master or doctoral degree). A demographic overview of the sample is presented in Table 1.

Table 2. Constructs, items and their descriptive statistics.

Constructs and items	M	SD
Trust perceptions (Cronbach’s alpha: 0.95)		
<i>In the fight against COVID-19, the government has decided to collect and use online personal data from citizens. In this regard, to what extent do you agree with the following statements:</i>		
1. The government is trustworthy in handling my personal data	4.19	1.57
2. The government tells the truth and fulfils its promises related to my personal data	4.15	1.53
3. I trust that the government keeps my best interest in mind when dealing with my personal data	4.49	1.64
4. The government is clear and consistent regarding the usage of my personal data	4.14	1.57
5. The government is honest with me when it comes to using my personal data	4.15	1.55
Risk beliefs (Cronbach’s alpha: 0.92)		
<i>In the fight against COVID-19, the government has decided to collect and use online personal data from citizens. In this regard, to what extent do you agree with the following statements:</i>		
1. In general, it is risky to give my personal data to the government	4.48	1.59
2. There is a loss of privacy associated with giving my personal data to the government	4.73	1.59
3. There is too much uncertainty with giving my personal data to the government	4.72	1.53
4. Providing the government with my personal data can involve unexpected problems	4.55	1.58
5. I don’t feel safe giving my personal data to the government	4.21	1.68
Privacy concern		
1. To what extent are you concerned about your online privacy when the government collects and uses your personal data in the fight against COVID-19	4.24	1.69
Support digital solutions		
<i>The government uses digital technologies in the fight against COVID-19. To what extent do you support the following digital solutions</i>		
1. Using digital technology (e.g. apps) to track people who may be infected or infect others.	4.11	1.77
2. The use of digital communication services such as WhatsApp by the government to quickly share information with the population	4.84	1.60
3. The use algorithms to determine which patients to prioritise in case of a shortage of healthcare capacity	3.40	1.79
4. Using Artificial Intelligence to find a drug/medicine against the coronavirus	5.15	1.49
5. Monitoring the use of mobile phones of citizens to check whether people are complying with the mandatory quarantine	3.82	1.83
6. Prevention of spreading disinformation about the coronavirus by means of automated analysis of social media posts	4.52	1.698

3.2. Measures

All items can be found in Table 2, along with their descriptive statistics. All instruments have been assessed on a 7-point scale from 1 (*strongly disagree*) to 7 (*strongly agree*). To measure trust perceptions, we used a validated instrument developed by Malhotra, Kim, and Agarwal (2004) consisting of five items. The items focus on the degree to which people believe that the government is trustworthy in handling and protecting their personal data. All items were averaged to form a single scale. Risk beliefs were assessed based on 7-point measure from the same authors (Malhotra, Kim, and Agarwal 2004). This scale consisted of five statements. The items focus on uncertainty and potential negative consequences of handing over personal data to the government. Scores on the five items were averaged to form a single scale for risk beliefs. Privacy concern was measured based on a single item, which has been adopted from prior studies (Chen and Chen 2015; Youn 2009). Respondents were asked to indicate the extent to which they were ‘concerned about their online privacy when the government collects and uses their personal data in the fight against Covid-19’. To measure respondents’ support for the digital solutions presented by the government, we asked respondents to indicate the extent to which they would support six different digital measures. These six solutions can be found in Table 2, and were discussed earlier in the theoretical framework.

3.3. Analytical strategy for clustering

To answer RQ1, a clustering method was used. Clustering is a commonly used exploratory data analysis technique to get a sense of the data structure. Although many clustering methods can be employed (e.g. hierarchical clustering, two-step clustering, etc.), we chose one of the most widely used cluster techniques: *K-means clustering* (Jain 2010). It refers to a robust and simple method to classify a sample of subjects based on a set of measured variables into a number of different groups or clusters so that similar subjects are placed in the same group (Cornish, 2007). The method starts with an initial guess for cluster centres, and each observation (i.e. respondent) is placed in the cluster to which it is closest. The cluster centres are then updated, and the entire process is repeated until the cluster centres no longer move (Charrad et al. 2014). A K-means cluster analysis is the recommended cluster solution when the dataset is moderate to large in size (e.g. large-scale surveys) (Brandtzæg, Heim, and Karahasanović 2011; Rogstad 2014).

In this analysis, K denotes the number of clusters, which must be specified *a priori* (Jain 2010; Pham, Dimov, and Nguyen 2005; Ray and Turi 1999). To determine the number of clusters, there are many different methods (see Kodinariya and Makwana 2013). In this study, we first started with two popular methods to visually inspect the clusters: the Silhouette method (Rousseeuw 1987) and the Gap Statistics method (Tibshirani, Walther, and Hastie 2001). The R-package *facto extra* (Kassambara and Mundt 2016) was used for this, which provides data visualisations for these methods. After this visual inspection, we used the R-package *NbClust* (Charrad et al. 2014), which computes 30 indices at once, in order to validate the optimal number of clusters. The results will be discussed in the next section.

4. Results

4.1. Cluster analysis

To answer RQ1, we need to segment respondents into clusters (based on K-means clustering) of individuals with distinctly different perceptions based on trust, risk and privacy concerns (RQ1). The Silhouette method and the Gap Statistic method both suggest 3 clusters as the optimal number. To cross-check this, we inspected the 30 indices provided by the *NbClust* R-package (Charrad et al. 2014). These indices revealed that 3 is the best number of clusters in our dataset (according to the ‘majority rule’). Therefore, we chose a three-cluster solution for our K-means cluster analysis. The identified clusters significantly differed in their trust perceptions, risk beliefs and privacy concerns (see Figure 1). Based on their scores on the three variables of interest, the three clusters are interpreted as (i) the *sceptical respondents*, (ii) the *carefree respondents*, and (iii) the *neutral respondents*. These groups will be discussed in the next paragraphs.

4.1.1. Cluster 1: the sceptical respondents

This first cluster accounts for 23% of the total sample ($N = 207$), which we named ‘sceptics’ because they stand out with their low level of perceived trust ($M = 2.22$), and considerably higher levels of risk beliefs ($M = 6.09$) and privacy concerns ($M = 6.01$). So out of the three clusters, this subgroup holds rather negative perceptions when it comes to the government collection their personal data in the fights against COVID-19.

4.1.2. Cluster 2: the carefree respondents

The second type of respondents that we identified are what we have called the *carefree* respondents, who account for around 29% of all respondents ($N = 267$).

These respondents are characterised by a high level of trust perception ($M = 5.26$), and much lower levels risk beliefs ($M = 3.11$) and privacy concern ($M = 2.06$). The results of this subgroup tend to indicate rather positive perceptions toward tracking in COVID-19 times, and therefore, is somewhat opposite to the sceptic respondents.

4.2. Cluster 3: the neutral respondents

The final cluster represents the largest subgroup with around 48% of all respondents ($N = 433$). These respondents have ‘neutral scores’ for trust ($M = 4.55$), risk ($M = 4.67$) and privacy concerns ($M = 4.75$), and these scores are not very different from each other. So, these respondents have rather neutral perceptions toward the governmental data tracking practices, without holding strong positive or negative views.

4.3. Features of the respondents from the three clusters

Table 3 displays the distribution of several demographic variables in the three clusters. All estimates also contain a superscript that presents the results of the (two-sided) significance testing of the group differences. All tests were adjusted using the Bonferroni correction.

An important result that emerges from the data is the significantly higher proportion of respondents in the 18–24 age category among the sceptics, in combination with significantly lower proportion in the 55+ category. This seems to indicate a trend in which sceptical respondents are more often younger people. Gender does not seem to differ significantly among the three subgroups. As for education, an interesting pattern can be discerned from Table 3. On the one hand, respondents with neutral perceptions (indifferent) are significantly overrepresented in the ‘lower education’ category as compared to the representation of this education level in the two other clusters. On the other hand, the proportion of higher educated respondents is significantly higher among the sceptical user group as compared to the two other groups. So, this seems to suggest that higher educational degree is more likely to be associated with sceptical perception, whereas lower educational degree with indifferent perceptions.

4.4. Support for technological measures of the government among the three clusters

The second research question (RQ2) was concerned with the relationship between the identified clusters and their support for digital solutions by the

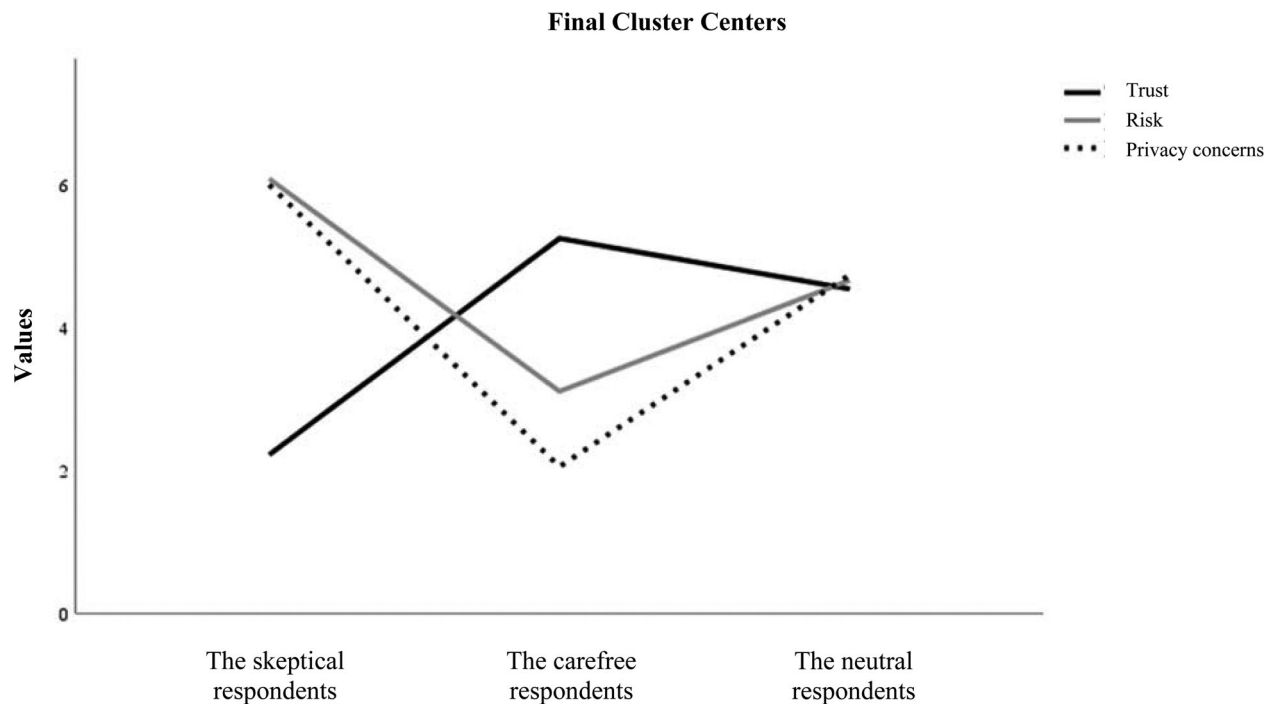


Figure 1. Three subgroups and their mean value on trust perception, risk beliefs and privacy concerns.

government. Pairwise comparisons between the clusters with Bonferroni correction are presented in Table 3.

These results show that sceptical respondents tend to have little support for technological measures. In fact, the *sceptic subgroup* has significantly lower support for *all* technological measures compared to the other two groups, except for ‘using AI for vaccine development,’ where sceptics have a support level similar to the neutral

group. A complete opposite pattern emerges from the data when it comes to the carefree respondents: they have significantly higher support for all digital solutions, except for one, i.e. using technology for monitoring quarantine compliance, where they have equal support levels as the neutral respondents. The neutral respondents can be positioned as somewhat in-between: they are more in support for digital solutions than the sceptical respondents, but less than the carefree people. So overall, these findings clearly indicate some meaningful differences between the three clusters, which will be further discussed in the general discussion.

Table 3. The cluster members’ distribution on several demographic characteristics.

	Sceptics (N = 207)	Carefree (N = 267)	Neutral (N = 433)
<i>Demographics</i>			
Age category (%)			
18–34	27.54 ^a	18.73 ^b	17.78 ^b
35–54	37.20 ^a	39.70 ^a	40.18 ^a
55+	35.27 ^a	41.57 ^b	42.03 ^b
Gender (%)			
Male	55.56 ^a	55.43 ^a	52.19 ^a
Female	44.44 ^a	44.57 ^a	47.81 ^a
Education (%)			
Low	16.43 ^a	22.85 ^b	31.87 ^c
Medium	52.17 ^{ab}	55.06 ^a	46.65 ^b
High	31.40 ^a	22.10 ^b	21.48 ^b
<i>Digital solutions</i>			
Each value represents the mean score of ‘support’ for the digital solution			
1. Proximity tracing	2.57 ^a	5.18 ^b	4.19 ^c
2. Public communication	4.09 ^a	5.00 ^b	4.53 ^c
3. Hospital management	2.58 ^a	4.66 ^b	3.89 ^c
4. Vaccine development	4.81 ^a	5.68 ^b	4.98 ^a
5. Quarantine compliance	2.83 ^a	3.76 ^b	3.45 ^b
6. Disinformation detection	4.32 ^a	5.39 ^b	4.75 ^c

Values within each row that have a different superscript differ significantly at least at $p < .05$ (Bonferroni correction).

5. General discussion

In this study, we first aimed to investigate how people evaluate the governmental practice of collecting data in the fight against the global pandemic. Drawing on the tenets of social contract theory (Dunfee, Smith, and Ross 1999), we investigated individuals’ trust, risk perceptions and privacy concerns, and by means of an exploratory cluster analysis of these factors introduced a typology consisting of three groups: the sceptical, the carefree, and the neutral respondents. It was found that each of the three groups exhibit unique characteristics. The *sceptical* respondents (23% of all respondents) are people with a high perceived risk and privacy concerns, in combination with a low degree of perceived trust when it comes to collecting their data. The *carefree*

respondents (29% of the respondents) have high levels of trust in governmental data collection, experience little risks, and have little privacy concerns. When we compare these two groups in terms of their composition, two interesting differences emerge. The group of sceptics has a significantly higher proportion of young people (18-34 years), as well as significantly higher educated people, whereas the carefree group consists of significantly more older people (55+years), as well as a significant higher amount of lower educated people.

When it comes to the educational differences, the findings confirm prior literature that higher educated tend to have higher privacy concerns and lower levels of trust toward online data collection practices (Malhotra, Kim, and Agarwal 2004; Sheehan 2002). With respect to age group differences, our findings challenge the argument that younger adults are less sceptic toward online data collection, and generally less concerned about their privacy in comparison to older adults (since our dataset revealed the opposite) (e.g. Halperin and Dror 2016; Quan-Haase and Ho 2020; Van den Broeck, Poels, and Walrave 2015). A possible explanation for this could be 'contextual integrity' (Nissenbaum 2010), which states that perceptions of privacy violations might depend on the specific context or circumstances in which data flows take place. In the case of COVID-19, it has been shown that young people are less likely to develop severe symptoms as compared to elderly (Liu et al. 2020). Therefore, younger adults might perceive personal data collection as more drastic and privacy-infringing (because of the lower severity of the disease among these individuals) compared to older cohorts. In other words, the characteristics of this specific context could be the reason why different age categories make different risk-benefits assessments about the government collecting their data. However, this explanation did not directly flow from our data, so it should be a subject of future empirical testing that assesses the role of context and perceived severity in perceptions related to data collection.

In future scholarly endeavours, it is important to have a more detailed overview of the underlying reasons of why a significant part of the population (23%) is sceptical about governmental data collection, which was beyond the scope of the present study. These sceptic perceptions of data collection could be a great barrier to the widespread adoption of digital solutions during a pandemic. Understanding why people are sceptical about their governments collecting data for rolling out technological tools is crucial, because it can contribute to a broader uptake of these technological solutions (Zhang et al. 2020). When it comes to the neutral respondents, we found that a large group (48%) of

people hold neutral levels of perceived trust, perceived trust, and privacy concerns with respect to governmental data collection. In terms of age distribution, this category is rather similar to the carefree group. However, when it comes to educational level, we see that this group of neutral respondents has significantly higher proportion of people with a lower education. Although it is important to explain this overrepresentation of lower educated people, it is difficult to do so because the 'neutral' group is rather ambiguous. It can be because they are ambivalent, undecided, unengaged, indifferent, or simply because they have not thought about it. From a scholarly perspective, it is important to obtain more fine-grained analyses to 'unpack' this 'central tendency' (i.e. neutral scores) to see whether there are additional variations in the responses of the public (e.g. ambivalence, see de Vries and Steenbergen 2013). From a societal perspective, with almost half of the population in this category (48% of the population), it places a great responsibility on governments to thoroughly understand these people when deploying new technologies and collecting data.

Personal data is at the heart of many digital solutions that European governments want to roll out in the fight against COVID-19 (Council of Europe 1990; Craglia et al. 2020). That is why this study also investigated to which extent the three identified groups support selected digital solutions presented by governments. On the one hand, we found that people with a sceptical mindset about the collection of their personal data by the government (i.e. sceptical subgroup) are more likely to have lower support for almost every technological solution on the digital agenda of the government. On the other, a carefree mindset (i.e. carefree subgroup) is associated with a higher level of support for the digital agenda of the government. So, people that evaluate governmental data collection in a neutral way when it comes to trust, risk and privacy, also tend to have moderate levels of support for specific digital solutions presented by that very same government. All in all, this suggests that the more certain people are in their social contract with the government (or lack of it), the more likely it is that this stance (positively or negatively) influences their support for the introduction of digital solutions by the government.

5.1. Theoretical and policy implications

From a theoretical perspective, this study makes an important contribution to the COVID-19 literature by showing that a *social contract* approach might help to understand and identify how people respond to collecting and using personal data in times of a pandemic.

Although other studies have already used this framework to explore people's perceptions about data collection and informational privacy (e.g. Culnan and Bies 2003; Fogel and Nehmad 2009; Malhotra, Kim, and Agarwal 2004; Martin 2012), this study shows that a social contract perspective can also be interesting in studying people's perceptions about how personal data is used and managed by the government with the goal of managing the COVID-19 crisis. In this respect, our results are also in line with the findings of Kruikemeier, Boerman, and Bol (2020), showing that trust beliefs, risk perceptions, and privacy concerns play a pivotal role in a mutual social contract. In addition, this study also contributes to the increasingly growing body of research on the technological responses to COVID-19 (e.g. Abuhammad, Khabour, and Alzoubi 2020; Albrecht et al. 2021; Lewandowsky et al. 2021; Oldeweme et al. 2021). Our findings confirm that perceptions about risk, privacy and trust are important considerations in accepting the digital solutions of a government during COVID-19; and in addition, can be used to create a typology of different subgroups within a population (i.e. the *sceptical*, the *carefree*, and the *neutral* individuals).

From a policy perspective, this study makes relevant contributions. Although data collection and usage for digital solutions are key in fighting the pandemic in an effective way, several concerns have recently been raised about the impact of these technologies on individual rights (e.g. privacy, data protection, personal autonomy) (Bengio et al. 2020). COVID-19 may have shifted the balance in data management and usage from individual rights towards the public good (Craglia et al. 2020). This has raised important questions about the *democratic legitimacy* of these data surveillance technologies (Craglia et al. 2020). As explained by Christensen and Læg Reid (2020), the question of governance legitimacy is about citizens' trust and support in their (democratic) government (in times of COVID-19), and includes concerns such as accountability and expectations. More precisely, it is about people trusting and supporting their government in deploying data-driven digital solutions. The contribution of this study is that it provides insights on the extent to which there is trust and support for governmental data collection and usage (i.e. the specific digital solutions), as well as information about which parts of the population that stand more behind these digital measures than others. Thanks to the cluster analysis, which provided an efficient segmentation approach that allowed to identify certain subgroups, policy makers can install targeted measures for these specific segments of the population.

In addition, one of the core debates in democratic legitimacy is the opinion of young people about their democratic government, with recent findings indicating a worrying increase in democratic dissatisfaction (see Foa et al. 2020). This might be a possible explanation why young people were found to be more sceptic and more concerned about their privacy with regards to governmental data collection (see 'contextual integrity' above). Therefore, it is important to keep track of and understand these dynamics in order to ensure youth legitimacy in times of a global pandemic. All in all, these findings could not only serve as a useful empirical basis for EU policy makers and regulatory bodies, but they also inform our understanding about the democratic legitimacy of these measures.

5.2. Limitations and future research

Finally, we also want to address some limitations that could inspire future research. First, this research is based on cross-sectional data. This means that it is not possible to articulate causal relationships. For instance, we found that trust, risk and privacy concerns are related to support levels of data-driven digital solutions, but we cannot claim that these perceptions directly enhance or undermine these digital solutions. Future research might therefore examine the causal structure of current findings. Second, data collection took place at one specific point-in-time, i.e. in the early days of the COVID-19 lockdown (April). It is not unlikely that perceptions in the context of data-driven technologies may change (in a positive or negative way) during the course of a crisis. Therefore, we also encourage scholars to explore whether current findings also hold at different points-in-time. Finally, as already mentioned earlier, we have a significant part of respondents that hold 'neutral' perceptions. Unfortunately, we do not have fine-grained data on why they scored neutral (it could be attributed to ambivalence, uncertainty, indifference, etc.; or, it can simply be a response bias whereby respondents avoid extreme answer categories). Future research might consider qualitative methods to obtain an in-depth understanding of people's neutral stance with regards to technology in times of COVID-19.

Acknowledgements

This study was commissioned by the research initiative 'Information, Communication & the Data Society' (ICDS) from the University of Amsterdam.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was funded by the Research Priority Area ‘Personalised Communication’ from the University of Amsterdam.

ORCID

Brahim Zarouali  <http://orcid.org/0000-0003-1042-4635>

Claes de Vreese  <http://orcid.org/0000-0002-4962-1698>

References

- Abuhammad, S., O. F. Khabour, and K. H. Alzoubi. 2020. “COVID-19 Contact-Tracing Technology: Acceptability and Ethical Issues of Use.” *Patient Preference and Adherence* 14: 1639–1647. doi:10.2147/PPA.S276183.
- Albrecht, R., J. B. Jarecki, D. S. Meier, and J. Rieskamp. 2021. “Risk Preferences and Risk Perception Affect the Acceptance of Digital Contact Tracing.” *Humanities and Social Sciences Communications* 8 (1): 1–9. doi:10.1057/s41599-021-00856-0.
- Altmann, S., L. Milsom, H. Zillessen, R. Blasone, F. Gerdon, R. Bach, F. Kreuter, D. Nosenzo, S. Toussaert, and J. Abeler. 2020. “Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study.” *JMIR MHealth and UHealth* 8 (8): e19857. doi:10.2196/19857.
- Baier, A. 1986. “Trust and Antitrust.” *Ethics* 96: 231–260.
- Bansal, G., F. M. Zahedi, and D. Gefen. 2010. “The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online.” *Decision Support Systems* 49 (2): 138–150. doi:10.1016/j.dss.2010.01.010.
- Bauer, P. C. 2014. “Conceptualizing and Measuring Trust and Trustworthiness.” *Committee on Concepts and Methods Working Paper Series* 61: 1–27.
- Bélanger, F., and L. Carter. 2008. “Trust and Risk in e-Government Adoption.” *The Journal of Strategic Information Systems* 17 (2): 165–176. doi:10.1016/j.jsis.2007.12.002.
- Beldad, A., M. de Jong, and M. Stehouder. 2011. “I Trust Not Therefore It Must be Risky: Determinants of the Perceived Risks of Disclosing Personal Data for e-Government Transactions.” *Computers in Human Behavior* 27 (6): 2233–2242. doi:10.1016/j.chb.2011.07.002.
- Bengio, Y., R. Janda, Y. W. Yu, D. Ippolito, M. Jarvie, D. Pilat, B. Struck, S. Krastev, and A. Sharma. 2020. “The Need for Privacy with Public Digital Contact Tracing During the COVID-19 Pandemic.” *The Lancet Digital Health* 2 (7): e342–e344. doi:10.1016/S2589-7500(20)30133-3.
- Brandtzæg, P. B., J. Heim, and A. Karahasanović. 2011. “Understanding the New Digital Divide—A Typology of Internet Users in Europe.” *International Journal of Human-Computer Studies* 69 (3): 123–138. doi:10.1016/j.ijhcs.2010.11.004.
- Budd, J., B. S. Miller, E. M. Manning, V. Lampos, M. Zhuang, M. Edelman, G. Rees, et al. 2020. “Digital Technologies in the Public-Health Response to COVID-19.” *Nature Medicine* 26 (8): 1183–1192. doi:10.1038/s41591-020-1011-4.
- Chan, E. Y., and N. U. Saqib. 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. doi:10.1016/j.chb.2021.106718.
- Charrad, M., N. Ghazzali, V. Boiteau, and A. Niknafs. 2014. “NbClust: An R Package for Determining the Relevant Number of Clusters in a Data Set.” *Journal of Statistical Software* 61 (6). doi:10.18637/jss.v061.i06.
- Chen, H.-T., and W. Chen. 2015. “Couldn’t or Wouldn’t? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection.” *Cyberpsychology, Behavior, and Social Networking* 18 (1): 13–19. doi:10.1089/cyber.2014.0456.
- Christensen, T., and P. Lægred. 2020. “Balancing Governance Capacity and Legitimacy: How the Norwegian Government Handled the COVID-19 Crisis as a High Performer.” *Public Administration Review*. doi:10.1111/puar.13241.
- Coleman, J. S. 1990. *Foundations of Social Theory*. Cambridge, Massachusetts: Harvard University Press.
- Cornish, R. 2007. “Statistics: cluster analysis.” *Mathematics Learning Support Centre*: 1–5.
- Council of Europe. 2020. *AI and Control of Covid-19 Coronavirus*. Artificial Intelligence. <https://www.coe.int/en/web/artificial-intelligence/ai-and-control-of-covid-19-coronavirus>.
- Craglia, M., S. de Nigris, E. Gómez-González, E. Gómez, B. Martens, M. Iglesias, M. Vespe, et al. 2020. *Artificial Intelligence and Digital Transformation: Early Lessons from the COVID-19 Crisis*. https://op.europa.eu/publication/manifestation_identifier/PUB_KJNA30306ENN.
- Culnan, M. J., and R. J. Bies. 2003. “Consumer Privacy: Balancing Economic and Justice Considerations.” *Journal of Social Issues* 59 (2): 323–342. doi:10.1111/1540-4560.00067.
- de Vries, C., and M. Steenbergen. 2013. “Variable Opinions: The Predictability of Support for Unification in European Mass Publics.” *Journal of Political Marketing* 12 (1): 121–141. doi:10.1080/15377857.2013.752654.
- Dowling, G. R., and R. Staelin. 1994. “A Model of Perceived Risk and Intended Risk-Handling Activity.” *Journal of Consumer Research* 21 (1): 119. <https://doi.org/10.1086/jcr.1994.21.issue-1>.
- Dunfee, T. W., N. C. Smith, and W. T. Ross. 1999. “Social Contracts and Marketing Ethics.” *Journal of Marketing* 63 (3): 14–32. doi:10.1177/002224299906300302.
- Economides, N. 2018. “The Theory of Social Contract and Legitimacy Today.” *Mediterranean Journal of Social Sciences* 9 (5): 19.
- European Commission. 2020. *JRC to Release AI Tech for Coronavirus Fact-Checkers*. EU Science Hub - European Commission, June 10. <https://ec.europa.eu/jrc/en/news/jrc-release-ai-tech-coronavirus-fact-checkers>.
- Foa, R. S., A. Klassen, D. Wenger, A. Rand, and M. Slade. 2020. *Youth and Satisfaction with Democracy: Reversing the Democratic Disconnect?* Centre for the Future of Democracy.
- Fogel, J., and E. Nehmad. 2009. “Internet Social Network Communities: Risk Taking, Trust, and Privacy

- Concerns.” *Computers in Human Behavior* 25 (1): 153–160. doi:10.1016/j.chb.2008.08.006.
- French, M., and T. Monahan. 2020. “Dis-ease Surveillance: How Might Surveillance Studies Address COVID-19?” *Surveillance & Society* 18 (1): 1–11. doi:10.24908/ss.v18i1.13985.
- Gasser, U., M. Ienca, J. Scheibner, J. Sleight, and E. Vayena. 2020. “Digital Tools Against COVID-19: Taxonomy, Ethical Challenges, and Navigation aid.” *The Lancet Digital Health* 2 (8): e425–e434. doi:10.1016/S2589-7500(20)30137-0.
- Halperin, R., and Y. Dror. 2016. “Information Privacy and the Digital Generation gap: An Exploratory Study.” *Journal of Information Privacy and Security* 12 (4): 166–180. doi:10.1080/15536548.2016.1243852.
- Jain, A. K. 2010. “Data Clustering: 50 Years Beyond K-Means.” *Pattern Recognition Letters* 31 (8): 651–666. doi:10.1016/j.patrec.2009.09.011.
- Kalliopi, A. D. 2016. “Privacy Decision-Making in the Digital Era.” Doctoral thesis, University of the Aegean.
- Kassambara, A., and F. Mundt. 2016. *R-package 'factoextra: Extract and Visualize the Results of Multivariate Data Analyses*. <https://cran.microsoft.com/snapshot/2016-11-30/web/packages/factoextra/factoextra.pdf>.
- Kodinariya, T. M., and P. R. Makwana. 2013. “Review on Determining Number of Cluster in K-Means Clustering.” *International Journal of Advance Research in Computer Science and Management Studies* 1 (6): 7.
- Kosterink, S. J., M. Hurmuz, M. den Ouden, and L. van Velsen. 2020. “Predictors to use Mobile Apps for Monitoring COVID-19 Symptoms and Contact Tracing: A Survey among Dutch Citizens.” *JMIR Formative Research*. doi:10.1101/2020.06.02.20113423.
- Kruikemeier, S., S. C. Boerman, and N. Bol. 2020. “Breaching the Contract? Using Social Contract Theory to Explain Individuals’ Online Behavior to Safeguard Privacy.” *Media Psychology* 23 (2): 269–292. doi:10.1080/15213269.2019.1598434.
- Lewandowsky, S., S. Dennis, A. Perfors, Y. Kashima, J. P. White, P. Garrett, D. R. Little, and M. Yesilada. 2021. “Public Acceptance of Privacy-Encroaching Policies to Address the COVID-19 Pandemic in the United Kingdom.” *PLOS ONE* 16 (1): e0245740. doi:10.1371/journal.pone.0245740.
- Liu, K., Y. Chen, R. Lin, and K. Han. 2020. “Clinical Features of COVID-19 in Elderly Patients: A Comparison with Young and Middle-Aged Patients.” *Journal of Infection* 80 (6): e14–e18. doi:10.1016/j.jinf.2020.03.005.
- Malhotra, N. K., S. S. Kim, and J. Agarwal. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model.” *Information Systems Research* 15 (4): 336–355. doi:10.1287/isre.1040.0032.
- Martin, K. E. 2012. “Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract.” *Journal of Business Ethics* 111 (4): 519–539. doi:10.1007/s10551-012-1215-8.
- Martin, K. E. 2016. “Understanding Privacy Online: Development of a Social Contract Approach to Privacy.” *Journal of Business Ethics* 137 (3): 551–569. doi:10.1007/s10551-015-2565-9.
- McDonald, S. M. 2020. “Technology Theatre and Seizure.” In *Data Justice and COVID-19: Global Perspectives*, edited by L. Taylor, G. Sharma, A. Martin, and S. Jameson, 20–27. London: Meatspace Press.
- Moon, Y. 2002. “Personalization and Personality: Some Effects of Customizing Message Style Based on Consumer Personality.” *Journal of Consumer Psychology* 12 (4): 313–325. doi:10.1016/S1057-7408(16)30083-3.
- Nam, T. 2019. “What Determines the Acceptance of Government Surveillance? Examining the Influence of Information Privacy Correlates.” *The Social Science Journal* 56 (4): 530–544. doi:10.1016/j.soscij.2018.10.001.
- Nissenbaum, H. F. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, California: Stanford Law Books.
- Okazaki, S., H. Li, and M. Hirose. 2009. “Consumer Privacy Concerns and Preference for Degree of Regulatory Control.” *Journal of Advertising* 38 (4): 63–77. doi:10.2753/JOA0091-3367380405.
- Oldeweme, A., J. Märtins, D. Westmattmann, and G. Schewe. 2021. “The Role of Transparency, Trust, and Social Influence on Uncertainty Reduction in Times of Pandemics: Empirical Study on the Adoption of COVID-19 Tracing Apps.” *Journal of Medical Internet Research* 23 (2): e25893. doi:10.2196/25893.
- Pavone, V., and S. D. Esposti. 2012. “Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-off Between Privacy and Security.” *Public Understanding of Science* 21 (5): 556–572. doi:10.1177/0963662510376886.
- Pham, D. T., S. S. Dimov, and C. D. Nguyen. 2005. “Selection of K in K-Means Clustering.” *Proceedings of the Institution of Mechanical Engineers, Part C: Journal of Mechanical Engineering Science* 219 (1): 103–119. doi:10.1243/095440605X8298.
- Quan-Haase, A., and D. Ho. 2020. “Online Privacy Concerns and Privacy Protection Strategies among Older Adults in East York, Canada.” *Journal of the Association for Information Science and Technology* 71 (9): 1089–1102. doi:10.1002/asi.24364.
- Ramelet, L. 2021. “A Contractual Justification for Strong Measures Against COVID-19.” *Public Philosophy Journal* 3: 1.
- Ray, S., and R. H. Turi. 1999. “Determination of Number of Clusters in K-Means Clustering and Application in Colour Image Segmentation”. *Proceedings of the 4th international conference on advances in pattern recognition and digital techniques*: 137–143.
- Razavi, S., C. Behrendt, M. Bierbaum, I. Orton, and L. Tessier. 2020. “Reinvigorating the Social Contract and Strengthening Social Cohesion: Social Protection Responses to COVID-19.” *International Social Security Review* 73 (3): 55–80. doi:10.1111/issr.12245.
- Redmiles, E. M. 2021. “User Concerns 8 Tradeoffs in Technology-Facilitated COVID-19 Response.” *Digital Government: Research and Practice* 2 (1): 1–12. doi:10.1145/3428093.
- Rogstad, I. D. 2014. “Political News Journalists in Social Media: Transforming Political Reporters Into Political Pundits?” *Journalism Practice* 8 (6): 688–703. doi:10.1080/17512786.2013.865965.
- Rousseuw, P. J. 1987. “Silhouettes: A Graphical aid to the Interpretation and Validation of Cluster Analysis.” *Journal of Computational and Applied Mathematics* 20: 53–65. doi:10.1016/0377-0427(87)90125-7.

- Sheehan, K. B. 2002. "Toward a Typology of Internet Users and Online Privacy Concerns." *The Information Society* 18 (1): 21–32. doi:10.1080/01972240252818207.
- Tang, Z., J. Y. Hu, and M. D. Smith. 2008. "Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor." *Journal of Management Information Systems* 24 (4): 153–173. doi:10.2753/MIS0742-1222240406.
- Thompson, N., T. McGill, A. Bunn, and R. Alexander. 2020. "Cultural Factors and the Role of Privacy Concerns in Acceptance of Government Surveillance." *Journal of the Association for Information Science and Technology* 71 (9): 1129–1142. doi:10.1002/asi.24372.
- Tibshirani, R., G. Walther, and T. Hastie. 2001. "Estimating the Number of Clusters in a Data Set via the gap Statistic." *Journal of the Royal Statistical Society: Series B (Statistical Methodology)* 63 (2): 411–423. doi:10.1111/1467-9868.00293.
- UN. 2020. *Digital Technologies Critical in Facing COVID-19 Pandemic*. UN DESA. United Nations Department of Economic and Social Affairs, April 15. <https://www.un.org/development/desa/en/news/policy/digital-technologies-critical-in-facing-covid-19-pandemic.html>.
- Van den Broeck, E., K. Poels, and M. Walrave. 2015. "Older and Wiser? Facebook Use, Privacy Concern, and Privacy Protection in the Life Stages of Emerging, Young, and Middle Adulthood." *Social Media + Society* 1 (2). doi:10.1177/2056305115616149.
- Voigt, S. 2021. "Contracting for Catastrophe: Legitimizing Emergency Constitutions by Drawing on Social Contract Theory." *Res Publica (Liverpool, England)*, doi:10.1007/s11158-021-09518-z.
- Warkentin, M., D. Gefen, P. A. Pavlou, and G. M. Rose. 2002. "Encouraging Citizen Adoption of e-Government by Building Trust." *Electronic Markets* 12 (3): 157–162. doi:10.1080/101967802320245929.
- Whitelaw, S., M. A. Mamas, E. Topol, and H. G. C. Van Spall. 2020. "Applications of Digital Technology in COVID-19 Pandemic Planning and Response." *The Lancet Digital Health* 2 (8): e435–e440. doi:10.1016/S2589-7500(20)30142-4.
- WHO. 2020. *Ethical Considerations to Guide the Use of Digital Proximity Tracking Technologies for COVID-19 Contact Tracing*. World Health Organization. https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1.
- Xu, F., K. Michael, and X. Chen. 2013. "Factors Affecting Privacy Disclosure on Social Network Sites: An Integrated Model." *Electronic Commerce Research* 13 (2): 151–168. doi:10.1007/s10660-013-9111-6.
- Youn, S. 2009. "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors Among Young Adolescents." *Journal of Consumer Affairs* 43 (3): 389–418. doi:10.1111/j.1745-6606.2009.01146.x.
- Zhang, B., S. Kreps, N. McMurry, and R. M. McCain. 2020. "Americans' Perceptions of Privacy and Surveillance in the COVID-19 Pandemic." *PLOS ONE* 15 (12): e0242652. doi:10.1371/journal.pone.0242652.
- Zivin, J. G., and N. Sanders. 2020. "The Spread of COVID-19 Shows the Importance of Policy Coordination." *Proceedings of the National Academy of Sciences* 117 (52): 32842–32844. doi:10.1073/pnas.2022897117.