

Tilburg University

Self-interest and data protection drive the adoption and moral acceptability of big data technologies

Kodapanakkal, Rabia I.; Brandt, Mark J.; Kogler, Christoph; Van Beest, Ilja

Published in:
Computers in Human Behavior

DOI:
[10.1016/j.chb.2020.106303](https://doi.org/10.1016/j.chb.2020.106303)

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

[Link to publication in Tilburg University Research Portal](#)

Citation for published version (APA):
Kodapanakkal, R. I., Brandt, M. J., Kogler, C., & Van Beest, I. (2020). Self-interest and data protection drive the adoption and moral acceptability of big data technologies: A conjoint analysis approach. *Computers in Human Behavior*, 108, [106303]. <https://doi.org/10.1016/j.chb.2020.106303>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.



Self-interest and data protection drive the adoption and moral acceptability of big data technologies: A conjoint analysis approach

Rabia I. Kodapanakkal^{*}, Mark J. Brandt, Christoph Kogler, Ilja van Beest

Tilburg University, the Netherlands

ARTICLE INFO

Keywords:

Moral acceptability
Big data
Conjoint analysis
Outcome favorability
Data protection
Data sharing

ABSTRACT

Big data technologies have both benefits and costs which can influence their adoption and moral acceptability. Prior studies look at people's evaluations in isolation without pitting costs and benefits against each other. We address this limitation with a conjoint experiment (N = 979), using six domains (criminal investigations, crime prevention, citizen scores, healthcare, banking, and employment), where we simultaneously test the relative influence of four factors: the status quo, outcome favorability, data sharing, and data protection on decisions to adopt and perceptions of moral acceptability of the technologies. We present two key findings. (1) People adopt technologies more often when data is protected and when outcomes are favorable. They place equal or more importance on data protection in all domains except healthcare where outcome favorability has the strongest influence. (2) Data protection is the strongest driver of moral acceptability in all domains except healthcare, where the strongest driver is outcome favorability. Additionally, sharing data lowers preference for all technologies, but has a relatively smaller influence. People do not show a status quo bias in the adoption of technologies. When evaluating moral acceptability, people show a status quo bias but this is driven by the citizen scores domain. Differences across domains arise from differences in magnitude of the effects but the effects are in the same direction. Taken together, these results highlight that people are not always primarily driven by self-interest and do place importance on potential privacy violations. The results also challenge the assumption that people generally prefer the status quo.

1. Introduction

Collecting data on a large scale is not new. Governments collect census data to estimate healthcare and education needs, meteorologists use data about past weather conditions to predict future weather conditions, and airlines use passengers' data of missed flights to predict future likelihood of missing flights to make sure flights do not fly partially empty (Clegg, 2017). It is the ease of processing, storing, and sharing data which has popularized the use of big data and the development of new technologies. Although there are benefits of using big data, ethicists argue that they can violate people's conventional sense of privacy and fairness (Barocas & Nissenbaum, 2014) and people indeed express these concerns (Pew Research Center, 2018). The costs and benefits of big data create situations where competing values and preferences are pitted against each other. In the present study, we systematically tested how people weigh competing factors that drive the willingness to adopt and how morally acceptable they find big data technologies.

Big data technologies have emerged in diverse domains, including law enforcement, healthcare, finance, retail, and human resources domains. In some U.S. cities, police use a new technology named 'Eye in the Sky' to continuously monitor an entire city. Through this technology, the police can access the exact time and location of a certain crime and track criminals easily (Mims, 2019). In the healthcare sector, doctors can remotely monitor patients through wearable devices ensuring better care during emergencies and significant cost reductions (Dunn, Runge, & Snyder, 2018; Raghupathi & Raghupathi, 2014). Financial institutions monitor peoples' spending habits and offer them monetary discounts (Williams, 2019). Similarly, supermarkets and department stores offer points and discounts to their customers by tracking what they buy (Mahmood, 2019). Big data technologies are not just about consumer decisions, but also whether one should be hired or not. Employers use algorithms that utilize data and performance of previously hired employees to select a suitable employee (O'Neil, 2016; Strom, 2019). Governments can take such technology to the next level and track their citizens' activities and consequently use this data via algorithms to

^{*} Corresponding author. Department of Social Psychology, Warandelaan 2, 5037 AB, Tilburg, the Netherlands.

E-mail address: r.i.kodapanakkal@tilburguniversity.edu (R.I. Kodapanakkal).

<https://doi.org/10.1016/j.chb.2020.106303>

Received 10 December 2019; Received in revised form 31 January 2020; Accepted 10 February 2020

Available online 11 February 2020

0747-5632/© 2020 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

rate their trustworthiness. For example, the Chinese government is assigning scores to citizens based on rules they follow or break by tracking their daily activities. These scores affect the citizens' ability to access services, travel, and obtain loans (Marr, 2019).

There are benefits to each of these technologies: they help stop crime, make healthcare and hiring procedures more efficient, and point consumers in the direction of cheaper products that they would like to buy. However, there are also downsides. Constant surveillance breaches innocent peoples' privacy (Mims, 2019). Assigning scores to employees and citizens through algorithms often mimic already existing biases, for instance against women and minority groups (Dastin, 2018; O'Neil, 2016) and are thus not equitable algorithms (Kleinberg & Mullainathan, 2018). Continuously monitoring patients can breach privacy and put sensitive data at risk if not protected properly.

Existing work suggests that people have mixed reactions to these technologies (e.g. Acquisti, Brandimarte, & Loewenstein, 2015; Debatin, Lovejoy, Horn, & Hughes, 2009). For example, more than 50% of Americans found it unacceptable to use algorithms for risk assessment of paroled criminals, for political campaigns, automated resume screening, analysis of job interviews, and computation of personal finance scores (Pew Research Center, 2018), but 80% found it acceptable to have social media sites use algorithms to recommend events happening around them. People are more likely to adopt healthcare technologies, but only when they have a chronic medical condition coupled with confidence in the system (Park & Shin, 2020). Others find that people will ignore privacy concerns when they receive hedonic (enjoyment of social interaction) or monetary benefits (Acquisti, John, & Loewenstein, 2013; Church, Thambusamy, & Nemati, 2017). People are also more likely to accept wearable technology if they find it useful and visible or noticeable by others (Chuah et al., 2016). These studies look at people's attitudes in isolation without considering tradeoffs, thus limiting the possibility of testing competing factors. We build on this work by examining how tradeoffs between different costs and benefits influence the adoption and evaluation of big data technologies. Crucially, this work will help map out the relative importance of people's concerns about big data.

1.1. Factors influencing the adoption and moral acceptability of big data technologies

To address this relative importance of costs and benefits, we use a conjoint design (Knudsen & Johannesson, 2018) and assess four factors that likely influence the adoption of big data technologies: *the status quo*, *outcome favorability*, *data sharing*, and *data protection*. We selected these four factors because they are relevant to both the benefits and costs of big data technologies and are the key factors in debates about big data technologies in the popular press (e.g., Clegg, 2017; Mims, 2019; O'Neil, 2016; Stephens-Davidowitz, 2017) and scientific literature (Barocas & Nissenbaum, 2014; Lyon, 2014). In the following sections, we explain in more detail about why each of these factors is potentially important and how a conjoint design helps in answering which factors have a relatively higher influence in the adoption and moral acceptability of these technologies.

1.1.1. Status quo

Status quo bias is the general preference for maintaining the current state of things and showing resistance to new options (Samuelson & Zeckhauser, 1988). People tend to stay with default options and evaluate them more favorably (Eidelman, Crandall, & Pattershall, 2009), even when the new option may be potentially more advantageous to them (Kahneman, Knetsch, & Thaler, 1991; Suri, Sheppes, Schwartz, & Gross, 2013). Just like in other contexts (Johnson & Goldstein, 2003; Spälti, Brandt, & Zeelenberg, 2017), we propose that people may show a status quo bias and could reject a new technology. Historical analyses suggest that people have always initially resisted new technologies and eventually find a balance between technological advancement and

maintaining social stability (Juma, 2016). Since big data technologies are fairly new and not the default, we expect people to adopt existing rather than new technologies and find the former more morally acceptable.

1.1.2. Outcome favorability

Outcome favorability is how personally beneficial an outcome of a technology is for the person making the decision, irrespective of whether this outcome is unfair to others or not (Krehbiel & Cropanzano, 2000). Most technologies come with benefits, but can also have costs for an individual or others in the society. However, if the outcome of these technologies is favorable to people, they may be willing to tradeoff the costs and find these technologies more morally acceptable. For example, people make judgments that are consistent with their own self-interest (De Benedictis-Kessner & Hankinson, 2019; Epley & Caruso, 2004; Weeden & Kurzban, 2017). In one study, people protested against sweatshop labor except when the product made directly benefitted them (Paharia & Deshpande, 2009). Similarly, we predict that people may be more likely to adopt and find a technology more morally acceptable if it provides a favorable outcome for them.

1.1.3. Data sharing

Data sharing is the extent to which the data collected by a technology is kept completely private or is shared with other parties. People often express concern about third parties that get access to their personal data. For example, there was public outrage after the personal Facebook data of US voters were used to target political advertisements for Donald Trump's election campaign (Cadwalladr & Graham-Harrison, 2018). Researchers have also found that a perceived privacy risk (using personal information or sharing it with other companies) lowers the adoption of mobile shopping apps (Chopdar, Korfiatis, Sivakumar, & Lytras, 2018). However, shared data could provide benefits in the long run. For instance, researchers could access medical records to develop new treatments (Tatonetti, Ye, Daneshjou, & Altman, 2012). This might be more acceptable by people than their data being shared for a political campaign. This suggests that people may selectively accept certain data-sharing practices depending on the precise identity of the third party (e.g., political parties vs. researchers). Since people generally tend not to trust third parties like pharmaceutical companies and corporations (e.g., Olsen & Whalen, 2009; Pew Research Center, 2019), we expect that people will be more likely to adopt and find those technologies more acceptable where their data is either not shared with third parties or shared with parties they are likely to trust.

1.1.4. Data protection

Another potential concern about big data use is how securely data is stored. Personal data can be misused, especially if it contains sensitive information about people's medical records, personal habits, or spending history. When asked broadly, people have expressed concern about giving up their privacy before big data was ubiquitous (Culnan & Armstrong, 1999). People have also expressed concern for data protection and security threats in the domain of internet surveillance (Poto-glou, Dunkerley, Patil, & Robinson, 2017). Whereas data sharing is about whether or not data will be shared with particular third parties, data protection is whether or not data will likely fall into the hands of malicious other parties without the consent of the use by the individual or organization collecting and storing the data. If corporations store data insecurely, there is a likelihood of the data being hacked and falling into the hands of cyber criminals. For example, in 2017 a data breach at Equifax led to the leak of sensitive credit information of nearly 143 million American consumers (McCandless, Evans, Barton, Tomasevic, & Geere, 2019). Data security can potentially send an important signal about the trustworthiness of an organization thus affecting people's willingness to adopt a new technology. We predict that people will be more likely to adopt a technology that stores peoples' data securely and also find it more morally acceptable.

1.2. The current study

Although we have predictions for each of these factors individually, we do not have a clear prediction for which factors would have more relative influence on the decision to adopt or reject a technology if they were pitted against each other. For example, some work suggests that people are motivated moral reasoners (Ditto, Pizarro, & Tannenbaum, 2009) and adopt moral positions that are in line with their self-interest (De Benedictis-Kessner & Hankinson, 2019; Epley & Caruso, 2004; Weeden & Kurzban, 2017). This suggests that outcome favorability would have an outsized role on the adoption and evaluation of big data technologies. Other work, however, suggests that people are largely risk averse (Harinck, Van Beest, Van Dijk, & Van Zeeland, 2012; Johnson & Slovic, 1995; Kahneman et al., 1991) including in their attitudes towards climate change (Fronzel, Simora, & Sommer, 2017). This would suggest that factors related to data protection or data sharing may be particularly important for predicting the adoption and evaluation of big data technologies. By using a conjoint design, we are able to evaluate which of the four factors has the largest influence when pitted against each other. For example, we can compare the effect of data protection with that of outcome favorability to see which of these has a higher relative influence on the adoption and moral acceptability of big data technologies. This allows for testing multiple hypotheses in a single design and also helps in understanding the relative support for the predictions for each factor.

The conjoint design we used asks participants to make multiple decisions about technologies and facilitates testing the causal effects of multiple factors simultaneously by systematically altering features of the technologies and testing which features have the strongest effect on decision-making (Bansak, Hainmueller, & Hangartner, 2016; Hainmueller, Hopkins, & Yamamoto, 2013). Conjoint designs have the following advantages over other approaches used to study concerns related to big data technologies: One, they enable us to directly compare the effects of the factors on evaluations with each other which is not possible when they are tested in isolation. Two, decisions in conjoint designs correspond with real-world behavior in representative samples (Hainmueller, Hangartner, & Yamamoto, 2015). Three, the conjoint design is a within-subject design that largely reduces the required sample size to achieve sufficient power compared to a between-subjects design. We expand on the traditional conjoint design, by collecting data for decisions about big data technologies in six different domains, from criminal investigations to banking and employment. This allows us to generalize our results to multiple technological domains unlike previous research that was mostly conducted in single domains and compare the results across domains.

2. Method

2.1. Participants

We conducted an online survey on MechanicalTurk using TurkPrime (Litman, Robinson, & Abberbock, 2017) with a total sample of 979 American participants (426 females, 447 males, and 106 people who did not indicate gender) ranging from 19 to 73 years of age ($M = 36.8$ years, $SD = 11.0$). Participants reported the number of MTurk surveys they completed in the last year (median of 700 surveys with an IQR of 1825 surveys). They also reported the amount of money they earned on MTurk in the last year (median of \$15 with an IQR of \$45). Although MTurk samples are not representative, experimental effects in MTurk samples correspond well to the same effects estimated in representative samples (Coppock, Leeper, & Mullinix, 2018).

We determined a sample size of 278 participants per domain based on the method proposed by De Bekker-Grob, Donkers, Jonker, and Stolk (2015) for conjoint designs. We first conducted the experiment among 100 participants and after checking that the data were being collected correctly in all conditions, we continued the data collection to reach 979

participants (we did not analyze the data until all data were collected). We had around 325 participants per domain. For a sensitivity power analysis, see supplemental materials. Participants who completed the survey partially were not excluded, only the incomplete trials were excluded from the analysis ($N_{\text{trials/domain}} \sim 3690$). We report all measures, manipulations, and exclusions in these studies. Participants received \$2.25 for completing the survey which lasted around 15 minutes.

2.2. Design and procedure

We created descriptions of six different emerging technologies. These covered surveillance (e.g., criminal investigations) and algorithmic (e.g., employment) uses of big data in both governments and the private sector. All of the technologies were based on existing or widely discussed technologies and the vignette descriptions were designed to be as neutral as possible (e.g., positive or negative implications were not emphasized). Each participant was randomly assigned to two of six technologies (~ 325 participants in each domain), one technology about surveillance and the other technology about algorithms. We also ensured that participants who saw one of the crime-related technologies were not also assigned to the other crime-related scenario.

We used an overarching between-participant vignette design for three conditions of status quo bias (brand new, new in your city but used elsewhere, and already in use) combined with a within-participant conjoint study design (12 trials per participant). We included three factors: *outcome favorability*, *data sharing*, and *data protection* in the conjoint design. It did not seem realistic to include the status quo in a within-subjects conjoint design because then each participant would have seen the same technology as both new and existing. We also decided to include a condition (new but used elsewhere) for status quo bias as there could be an inclination to adopt a technology if its portrayed as being used somewhere else already.

Fig. 1 provides an overview of the study. Participants first completed the vignette design. Participants read a basic explanation of how the technology operates and its main goal (see supplemental materials). Embedded in this description was the status quo manipulation, where we randomly assigned participants to one of three different conditions based on whether 1) the technology was brand new, 2) the technology was new to their city/neighborhood but had been used in other places, and 3) the technology had been in use for the last few years in their city/neighborhood. For example, participants who were assigned to the employment domain read the following text (the three status quo conditions are written in bold):

“You are planning to apply for a job at Company X. This company is considering using a **brand new/new/an** algorithm to screen new job applicants.

This technology has never been used before /This technology is being used by employers in other countries/ This technology has been in use for a few years in your country.

This algorithm will rely on the data of employees’ qualifications, demographics, and geographical location to predict which applicants are likely to stay at the job long term or quickly quit the job.”

After reading these initial descriptions containing the status quo manipulation, participants were asked to rate their emotional responses to this technology on a scale of 0–100. As these measures are not the main focus of this manuscript, we present the results relevant to emotions only in the supplemental materials.

Next, all participants completed the conjoint experimental design (see Fig. 1b) which used within-participant manipulations to test the three factors: outcome favorability, data sharing, and data protection. We presented participants with two versions of the technology (Version A and Version B) across 12 trials in a random order with the task of choosing their preferred technology. Both versions contained

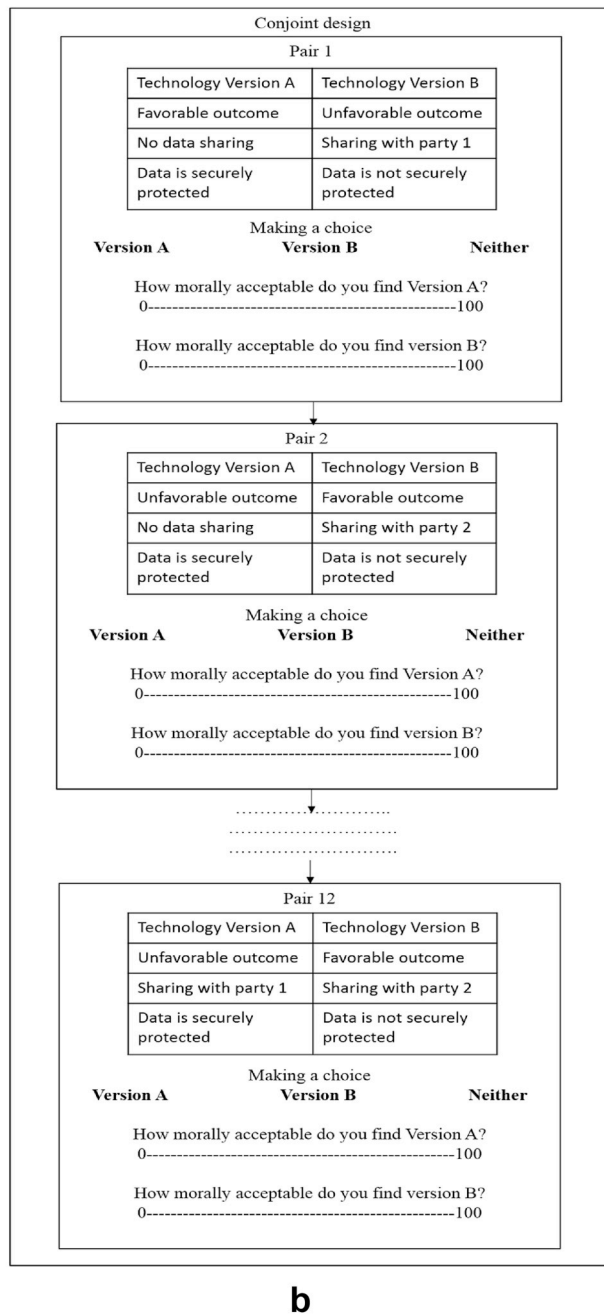
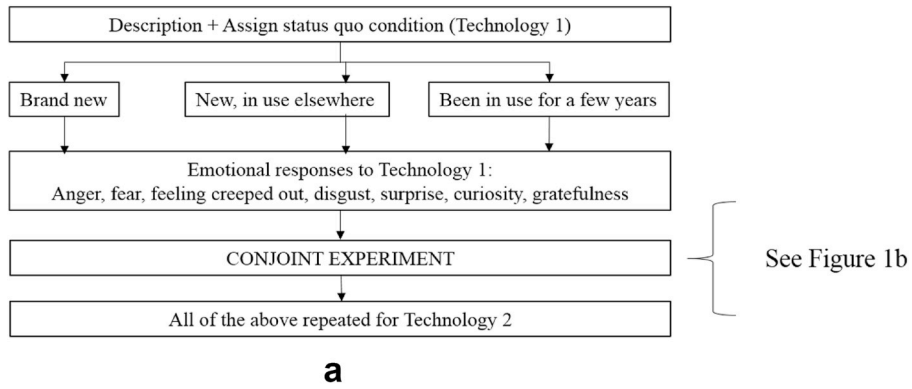


Fig. 1. a. Flowchart displaying the procedure of the study. Participants were randomly assigned to one of the status quo conditions. b. Flowchart displaying the conjoint design within the study. Within the conjoint, participants completed 12 trials for each technology and each participant did so for two technologies.

information about the three factors. Each factor consisted of two or three levels which were randomly assigned to each version in each trial (see Table 1). Outcome favorability had two levels: favorable outcome and unfavorable outcome. Data sharing had three levels: no sharing with a third party and data sharing with two different parties. These different parties included more or less trusted institutions. Data protection had two levels: encrypted secure data and non-encrypted non-secure data. We used three levels for data sharing instead of two as we wanted to see whether people are willing to share their data with some third parties and not with others or whether they prefer not sharing their data at all. Across the 12 trials, we presented participants with all possible combinations of levels between the factors. The levels of each factor were randomly varied and the combinations for each trial were different. For example, if Version A had a favorable outcome, then Version B had an unfavorable outcome.

2.2.1. Dependent variables

In each trial, participants were asked to 1) choose which version (A

or B) they preferred including a third option to choose neither version, and 2) rate the moral acceptability of version A and version B (see Figs. 1b and 2). On a scale of 0–100, participants answered the question: “How would you morally evaluate Technology Version A/B (where 0 is morally unacceptable and 100 is morally acceptable)”.

This entire process was repeated for the second technology after which participants answered some demographic questions related to age, gender, political orientation, education level, and experience on MechanicalTurk.

3. Results

3.1. What is the relative contribution of the status quo, outcome favorability, data sharing, and data protection towards the adoption of a technology?

3.1.1. Analytical approach

To answer this question, we performed mixed effects logistic

Table 1
Factors and levels used in the conjoint for all technologies.

Government-related domains			
Factors	Levels		
Domain: Criminal investigations			
Outcome favorability	This technology increases the rate of crime solving in your neighborhood	This technology decreases the rate of crime solving in your neighborhood	
Data sharing	Police use the data and do not share it with anyone	Police work with other governmental institutions and share data with them	Police work with the private company that made the technology and share data with them
Data protection	Data is encrypted and stored securely	Data is not encrypted and not stored securely	
Domain: Crime prevention			
Outcome favorability	Based on this algorithm, there is a lower chance that the police would stop and interrogate someone in your neighborhood including you.	Based on this algorithm, there is a higher chance that the police would stop and interrogate someone in your neighborhood including you	
Data sharing	Police use the data and do not share it with anyone	Police work with other governmental institutions and share data with them	Police work with the private company that made the technology and share data with them
Data protection	Data is encrypted and stored securely	Data is not encrypted and not stored securely	
Domain: Citizen score			
Outcome favorability	Based on this technology, your trust score is likely to be higher than the average score in the neighborhood	Based on this technology, your trust score is likely to be lower than the average score in the neighborhood	
Data sharing	The government works alone and your data is not shared with anyone else	The government works with a private company and shares data with them	The government works with academic researchers and shares data with them
Data protection	Data is encrypted and stored securely	Data is not encrypted and not stored securely	
Private domains			
Factors	Levels		
Domain: Healthcare			
Outcome favorability	This technology increases likelihood of saving patients' lives in an emergency	This technology decreases likelihood of saving patients' lives in an emergency	
Data sharing	Medical practitioners use the data and do not share it with anyone	Medical practitioners may share the data with pharmaceutical companies	Medical practitioners may share the data with academic researchers
Data protection	Data is encrypted and stored securely	Data is not encrypted and not stored securely	
Domain: Banking			
Outcome favorability	This technology increases your chances of receiving a discount	This technology decreases your chances of receiving a discount	
Data sharing	The bank uses the data and does not share it with anyone	The bank may share the data with governmental institutions	The bank may share the data with other private companies
Data protection	Data is encrypted and stored securely	Data is not encrypted and not stored securely	
Domain: Employment			
Outcome favorability	This technology increases the chances of someone from your neighborhood finding employment	This technology decreases the chances of someone from your neighborhood finding employment	
Data sharing	Employers work alone and do not share the data with anyone	Employers work with a private company and share data with them	Employers work with academic researchers and share data with them
Data protection	Data is encrypted and stored securely	Data is not encrypted and not stored securely	

Note: In all domains, the level with the unfavorable outcome, with no data sharing, and with no data protection were chosen as reference categories for dummy coding.

You are currently viewing PAIR 1. Please read the information about both versions carefully before answering the questions below.

Technology version A	Technology version B
This technology increases the chances of finding employment for someone from your neighborhood including you	This technology decreases the chances of finding employment for someone from your neighborhood including you
The company works with academic researchers and shares data with them	The company works with other private companies and shares data with them
Data is encrypted and stored securely	Data is not encrypted and not stored securely

If you have to make a choice between these versions of the technology, which one would you choose?

Technology version A

Technology version B

Neither of these

On a scale of 0 to 100, how would you morally evaluate Technology version A?
(where 0 is *morally unacceptable* and 100 is *morally acceptable*)

(click on the slider to make your choice)

Morally unacceptable
0
10
20
30
40
50
60
70
80
90
100
Morally acceptable

Technology version A

On a scale of 0 to 100, how would you morally evaluate Technology version B?
(where 0 is *morally unacceptable* and 100 is *morally acceptable*)

(click on the slider to make your choice)

Morally unacceptable
0
10
20
30
40
50
60
70
80
90
100
Morally acceptable

Technology version B

Fig. 2. This is an example of one trial in the conjoint. Participants view the table which shows two versions of the same technology. The three rows give them information about various factors. In each trial, a new combination of the information is presented to the participants and over 12 trials, participants provide choices and moral acceptability ratings for all possible combinations.

regressions, where we regressed the dependent variable (DV) of adoption of technology onto the four factors. We dummy coded this DV where participants either opted for Version A, Version B, or neither of the versions. The option that participants chose in a particular trial was coded as 1 and the remaining two options were assigned as 0. For example, when participants chose Version A, then response for Version A was coded as 1 and responses for Version B and Neither Version were coded as 0. When participants chose Version B, then this response was coded as 1 and the other two options were coded as 0. When participants chose Neither Version, this response was coded as 1 and the remaining two were coded as 0. We assigned reference categories to each of the four factors. For status quo, there were three levels: the technology is brand new, new but used in other cities (new but used), and already being used (status quo). The last condition was used as a reference category. For outcome favorability, data sharing, and data protection, the unfavorable outcome level, the level where no data was shared with any party, and the non-encrypted non-secure data protection level were used as the respective reference categories.

We estimated the main effects of the factors on adoption of technologies. Because the status quo is manipulated between-subjects, the coefficients for the status quo represent the likelihood participant select either of the technologies (Version A or Version B) compared to not selecting any technologies. For all of the other factors the coefficients represent the likelihood of choosing the version (Version A or Version B) with one level (e.g., data protection) compared to the version with the other level (e.g., no data protection). In the first mixed logistic regression model, we estimated the average effect of each factor on the adoption of the technologies across all domains with the responses nested within both participants and domains. In the second mixed logistic regression model, we estimated the effects of the factors separately for each domain with the responses nested only within participants. The first model gives us an average estimate across domains, whereas the second model gives us specific estimates for each domain. In both these analyses, we obtained values of how much the probability of acceptance (change in probability) increased or decreased when one factor was present over the other. Details of the results (estimates and CIs) are available in Figs. 3 and 4 and in the supplemental materials. In the supplemental materials, we also report separate models that estimated how these factors interact with each other for both adoption and moral

acceptability. These models did not change the conclusions reported here and so we only report the main effects in the manuscript.

3.1.1.1. Average estimate. The first model showed that among the three factors in the conjoint design, outcome favorability and data protection had a relatively higher influence on decisions to adopt or reject technologies averaged across all of the domains (see Fig. 3). The likelihood of adopting a technology increased by 32.1% [31.3, 32.8] when the outcome was favorable and increased by 31.3% [30.6, 32.1] when the data was protected. On average, sharing data with third parties significantly lowered the probability of adoption by approximately 10%. Contrary to our predictions, when a technology was “brand new” or “already in use”, it did not affect adoption (−0.8% [−1.9, 0.1]); however, people in the “new but used elsewhere” conditions were 1.8% [0.9, 2.9] less likely to adopt the technology than in the “already in use” condition. The effects of the status quo for these comparisons were significant, but small.

3.1.1.2. Estimates for each domain. In the second model, we estimated change in probabilities for each domain separately (see Fig. 4). In the domain of criminal investigations and employment, both favorable outcomes and data protection had a similar relative influence on the adoption of the technology. In the crime prevention, citizen scores, and banking domains, data protection was the dominating factor and the likelihood of adopting a technology increased when the data was protected compared to other factors. In the healthcare domain, outcome favorability was the clear dominating factor. Sharing data with third parties lowered the probability of adoption in all domains. Although a small effect emerged in the first model, when analyzed separately, there was no effect of status quo in any of the domains.

3.1.2. Comparisons between domains

Using the estimates in each domain, we did pairwise comparisons and calculated z-scores to test whether the effects were in the same direction and if the magnitudes of the effects were similar or different across domains (see Table 2). The direction of the effects (for all significant effects) were the same in all domains for outcome favorability, data protection, and data sharing (effects of status quo were not significant) (see ‘Direction of effects’ heading in Table 2). Although the

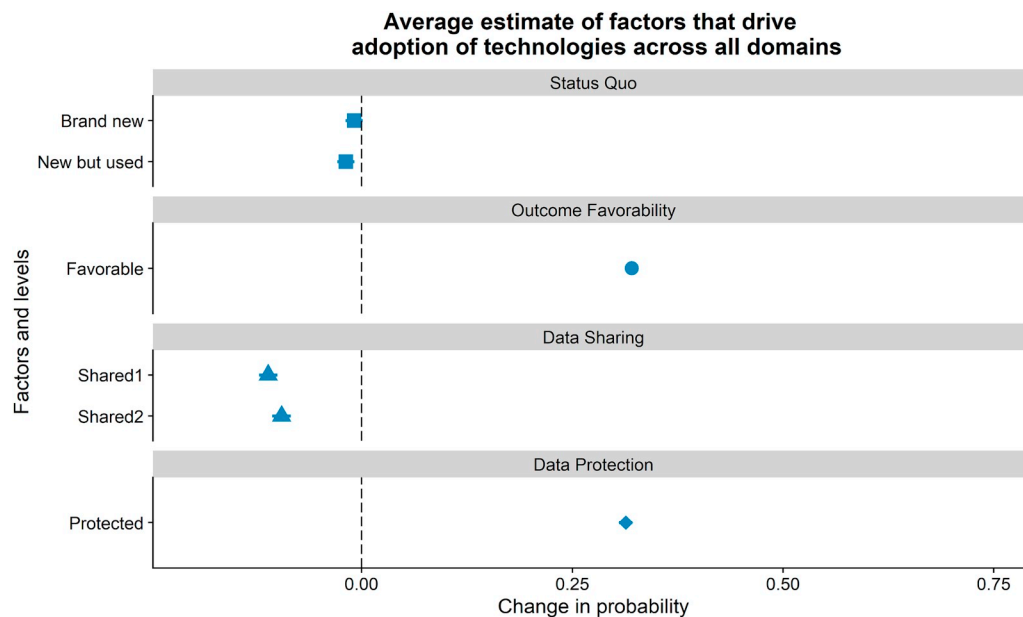


Fig. 3. This plot represents the average estimate (main effects) for the relative influence of status quo, outcome favorability, data sharing, and data protection on the adoption of big data technologies. The x-axis represents the change in probability of the factor level selected. The y-axis represents the four factors and their respective levels. The error bars denote 95% confidence intervals. Used, Not favorable, Not shared, and Not protected are the reference categories.

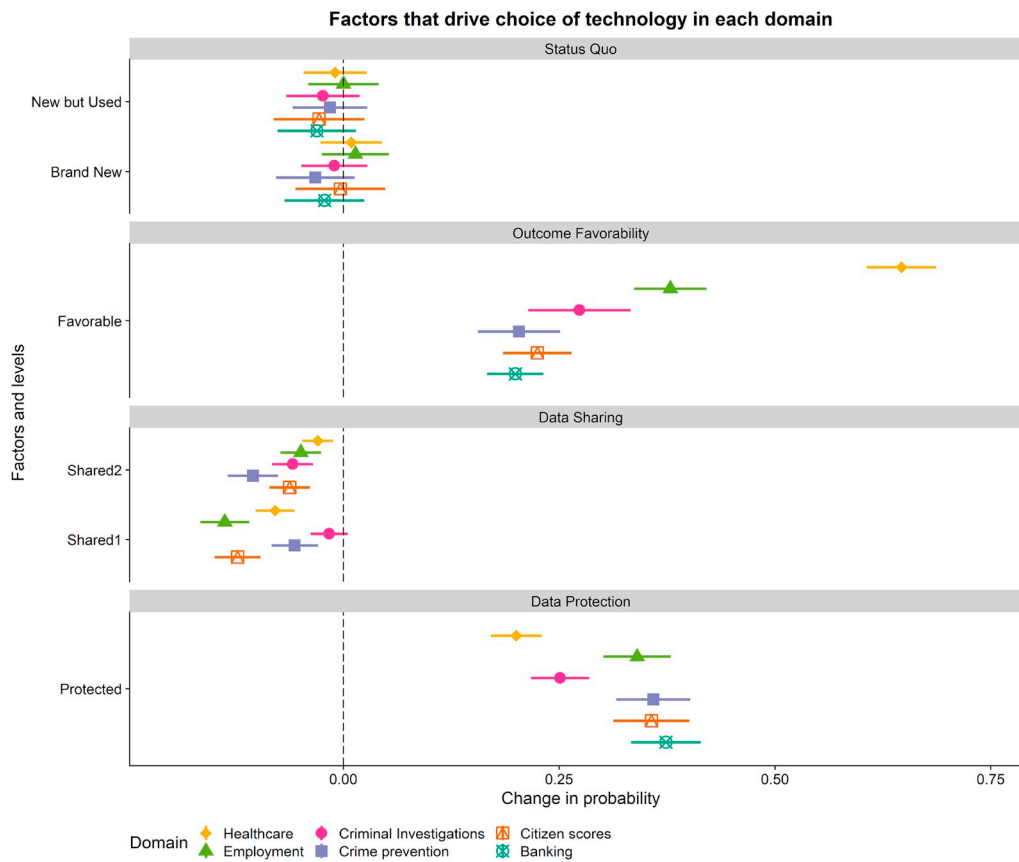


Fig. 4. This plot represents the estimates (main effects) for the relative influence of status quo, outcome favorability, data sharing, and data protection on the adoption of big data technologies for each domains. The x-axis represents the change in probability of the factor level selected. The y-axis represents the four factors and their respective levels. The error bars denote 95% confidence intervals. Used, Not favorable, Not shared, and Not protected are the reference categories.

directions of the effects were similar, the magnitude was not (see significant magnitude comparisons in Table 2). Outcome favorability was different in magnitude for ~85% of the pairwise comparisons. Approximately 65% of the comparisons were different in magnitude for

data protection and ~75% were different in magnitude for data sharing. For status quo, the magnitudes were not different for all pairwise comparisons.

To summarize, on average, outcome favorability, data protection,

Table 2
Comparison of effects on decisions to adopt technology across all domains.

Comparison between:		Factors and levels					
		Status Quo		Outcome favorability	Data sharing		Data protection
Brand new	New, but used elsewhere	Favorable outcome	Shared with party 1	Shared with party 2	Data is secure		
		Direction of effects					
		-	-	6/6	5/6	6/6	6/6
First domain	Second domain	Magnitude comparison (z-scores)					
Criminal investigations	Healthcare	-0.75	-0.54	-29.73***	3.74***	-1.93	4.05***
Criminal investigations	Banking	0.32	0.25	5.68***	10.66***	9.19**	-9.35***
Criminal investigations	Crime prevention	0.70	-0.29	5.13***	2.24*	2.54**	-7.90***
Criminal investigations	Employment	-0.85	-0.79	-7.88***	7.50***	-0.43	-6.68***
Criminal investigations	Citizen score	-0.19	0.14	3.69***	6.49***	0.24	-8.03***
Healthcare	Banking	1.03	0.76	38.49***	7.93***	12.35***	-14.91***
Healthcare	Crime prevention	1.44	0.19	36.22***	-1.38	4.81***	-12.97***
Healthcare	Employment	-0.14	-0.29	22.51***	4.44***	1.54	-11.77***
Healthcare	Citizen score	0.44	0.59	36.11***	3.26**	2.34*	-13.40***
Banking	Crime prevention	0.35	-0.51	-0.34	-8.60***	-6.78***	1.14
Banking	Employment	-1.12	-0.99	-14.37***	-3.14**	-10.06***	2.67**
Banking	Citizen score	-0.46	-0.09	-2.10*	-4.45***	-9.55***	1.37
Crime prevention	Employment	-1.51	-0.45	-13.41***	5.39***	-3.08**	1.43
Crime prevention	Citizen score	-0.79	0.38	-1.66	4.31***	-2.44*	0.17
Employment	Citizen score	0.54	0.81	12.26***	-1.21	0.71	-1.32

Note: Similar direction of effect shows the number of domains per the total number of domains where the effect is significant and in the same direction. The remaining domains were not significant. Each column denotes factors and their levels. Below these, each row is a pairwise magnitude comparison showing z-scores using differences of the effect estimates found in different domains. To denote significance levels: $p < .05$, $**p < .01$, $***p < .001$.

and data sharing, all had an effect on adoption of technologies. The relative influence of both outcome favorability and data protection was higher than data sharing but between the two, there was no clear dominant factor. Although the average estimate showed that both outcome favorability and data protection had a similar influence on adoption, estimates in each domain showed that the dominating factor varied in different domains. By further comparing the domains, we found that there was a general directional trend in the effects of the factors on adoption, although the sizes of the effects in each domain were quite different.

3.2. How are status quo, outcome favorability, data sharing, and data protection factors related to the moral acceptability of the technologies?

3.2.1. Analytical approach

We dummy coded the four factors: status quo, outcome favorability, data sharing, and data protection similar to the previous section on adoption of the technologies. Since the dependent variable of moral acceptability ranged from 0 to 100 (non-binary values), we used a linear mixed effects design with moral acceptability as the dependent variable, status quo, outcome favorability, data sharing, and data protection, as fixed factors, and participant ID, trial number, and domain (in case of average estimates) as random factors. We estimated the main effects of the factors on moral acceptability of the technology. Because the status quo is manipulated between-subjects, the coefficients for the status quo represent the average moral acceptability of the technologies (Version A and Version B) across all of the trials. For all of the other factors the coefficients represent the difference in moral acceptability between the version (Version A or Version B) with one level (e.g., data protection) compared to the version with the other level (e.g., no data protection).

In the first mixed regression model, we estimated the average effect of each factor on the moral acceptability across all domains with responses nested within both participants and domains. In the second mixed model, we estimated the effects of the factors separately for each domain with responses nested only within participants. For all estimate values and CIs, refer to Figs. 5 and 6 and the supplemental materials.

3.2.1.1. Average estimate. The first model showed that among the four factors, on average across domains, data protection had the highest relative influence on moral acceptability of the technologies compared to outcome favorability and data sharing (see Fig. 5). On average, sharing data with third parties significantly lowered the moral acceptability of the technologies. In line with our predictions, people in the

status quo condition, where the technology was already in use, were most likely to find the technologies morally acceptable.

3.2.1.2. Estimate for each domain. The results from the second model showed that in five out of six domains, data protection was the driving factor of moral acceptability i.e. participants were more likely to rate the technology as morally acceptable when their data was protected. Only in the healthcare domain, outcome favorability was the driving factor with participants more likely to find the technology morally acceptable when it had a favorable outcome. In all domains, when data was shared with third parties, participants found the technology less morally acceptable. However, data sharing influenced moral acceptability to a lesser extent than outcome favorability and data protection. Although the average estimate showed a status quo bias, the citizen score domain was the only domain where there was a status quo bias i.e., people found the technology less morally acceptable when it was new rather than already in use. In all other domains, there was no effect of status quo on moral acceptability of the technologies.

3.2.2. Comparison between domains

Similar to adoption of technologies, we further compared the direction and magnitude of the four factors driving moral acceptability across the six domains (see Table 3). We found that across all domains, the effects (all significant effects) were in the same direction (see ‘Direction of effects’ heading in Table 3). However, the magnitude of the effects differed (see significant magnitude comparisons in Table 3). Outcome favorability was different in magnitude for all comparisons except the one between crime prevention and banking domains (~95% of all comparisons). 80% of the comparisons were different in magnitude for data protection and around 65% different in magnitude for data sharing. For status quo, only 20% of the comparisons were different in magnitude.

To summarize, all four factors had an influence on the moral acceptability of the technologies with data protection showing the highest relative influence. Unlike the adoption of technologies, the evaluation of moral acceptability seemed more consistent in terms of which factor (data protection) was dominant. Although the average estimate showed a status quo bias, on further investigation into the individual domains, we found that this effect was only present in the citizen scores domain and not any of the others. By further comparing the domains, we found that the effects were in the same direction in all domains although the magnitudes of the effects in each domain were quite different.

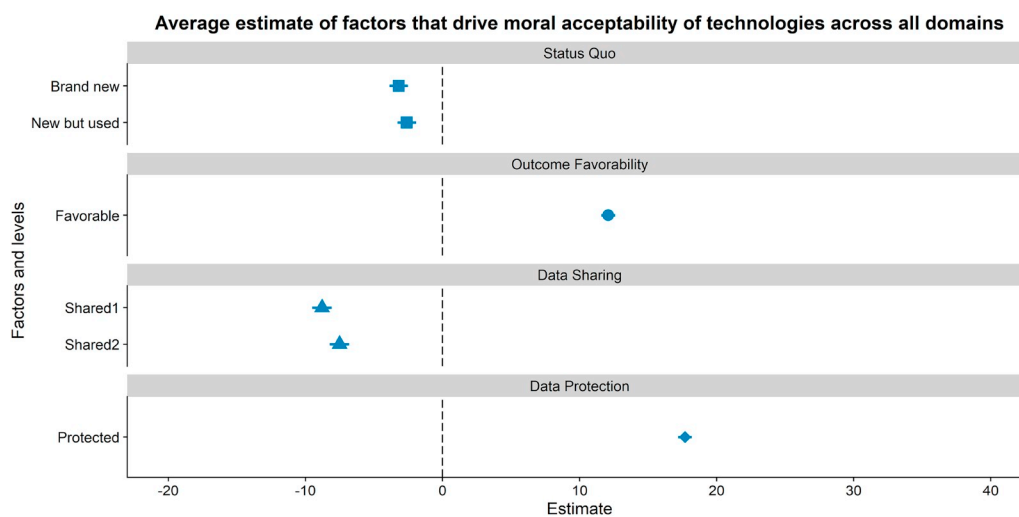


Fig. 5. This plot represents the average main effects of a linear mixed effects model on moral acceptability of technologies. The x-axis represents the coefficient estimate with zero being the reference category. The y-axis includes the various factors and their levels that were tested in the model. The error bars denote 95% confidence intervals. Used, Not favorable, Not shared, and Not protected are the reference categories.

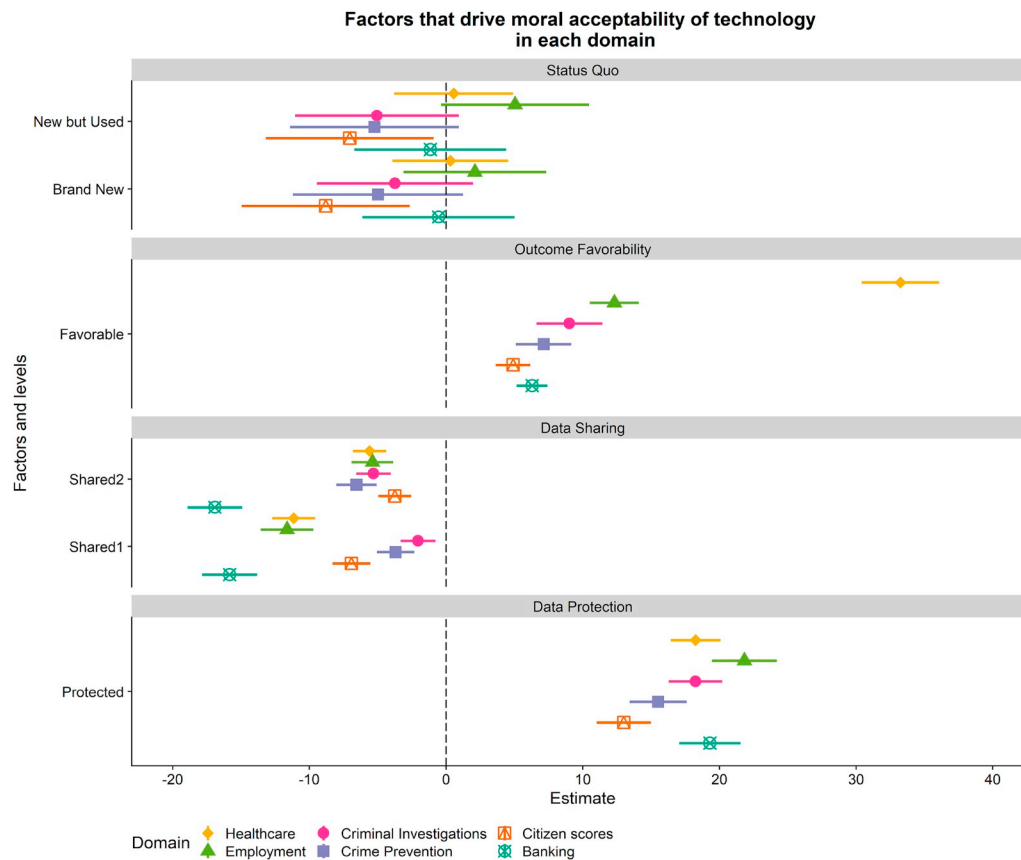


Fig. 6. This plot represents the main effects of a linear mixed effects model with separate estimates for each domain on moral acceptability of technologies. The x-axis represents the coefficient estimate with zero being the reference category. The y-axis includes the various factors and their levels that were tested in the model. The error bars denote 95% confidence intervals. Used, Not favorable, Not shared, and Not protected are the reference categories.

4. Discussion

We used a conjoint design to examine the relative influence of the status quo, outcome favorability, data sharing, and data protection on the adoption of big data technologies and their moral acceptability in six domains: criminal investigations, crime prevention, citizen scores, healthcare, banking, and employment. We found that outcome favorability, not sharing data with third parties, and data protection, all influenced the adoption of technologies and their moral acceptability. However, outcome favorability and data protection were the dominant factors and on average, had a similar relative influence on the adoption of technologies. Analyses for each domain separately showed that outcome favorability had a stronger influence in the healthcare domain, data protection had a stronger influence in the banking, crime prevention, and citizen score domains, and both factors had a similar influence in the criminal investigations and employment domains. On average, as well as in five out of six domains (except healthcare), data protection was the strongest driver of moral acceptability.

Contrary to our predictions, status quo did not drive the adoption or rejection of the technologies. On average, people showed a small effect opposite to our predictions, thus not preferring the status quo. On the other hand, for the moral acceptability variable, on average people in the status quo condition were more likely to find the technologies morally acceptable. However, this effect was only found in the citizen scores domain. It is possible that participants especially did not like this domain. People scored relatively higher on negative emotional reactions and very low on gratefulness in the citizen score domain compared to other domains (see supplemental materials). Negative emotions have also been generally associated with unsuccessful acceptance of technologies (Partala & Saari, 2015). Thus, they may have found the

implementation of a (brand) new technology in this domain less morally acceptable compared to one that already exists. Overall, the results suggest that the status quo is not an important factor for understanding the acceptance of big data technologies.

Although the magnitudes of effect of the factors were slightly different for each domain, we did find that the direction of the effects was the same for most factors in all six domains illustrating that these findings can be generalized to various domains. The basic description of the technologies all involved some level of privacy invasion and people reported feeling creeped out, scared, and angry towards these technologies (see supplemental materials), but when given a choice people were still more likely to choose some version of the technology than neither. This was surprising as there is evidence to show that people express concerns about privacy violations (Acquisti et al., 2015; Pew Research Center, 2018).

4.1. Healthcare domain: an outlier

Among all domains, the healthcare domain seemed to be an outlier. In this domain, we found a stronger effect of outcome favorability on the decision to adopt the technology and its moral acceptability compared to the other domains. This particularly strong effect may be because the favorable outcome in this case was saving lives, which is likely more fundamental compared to the favorable outcomes in the other domains (e.g., receiving a discount, getting a job). This is in line with the research done on the framing effect (Tversky & Kahneman, 1981) which shows that people respond more strongly to human lives being at stake rather than other contexts. However, there may be other reasons for differences in the healthcare domain. In the current study, the emotional reactions towards the technology which were recorded before people were

Table 3
Comparison of effects on moral acceptability of technology across all domains.

Comparison between:		Factors and levels					
First domain	Second domain	Status Quo		Outcome favorability	Data sharing		Data protection
		Brand new	New, but used elsewhere	Favorable outcome	Shared with party 1	Shared with party 2	Data is secure
Direction of effects							
		1/6 (rest are n.s.)	1/6 (rest are n.s.)	6/6	6/6	6/6	6/6
Magnitude comparison (z-scores)							
Criminal investigations	Healthcare	-1.19	-1.66	-34.65***	9.55***	0.70	-0.02
Criminal investigations	Banking	-0.82	-1.03	4.23***	16.17***	13.42***	-1.63
Criminal investigations	Crime prevention	0.14	-0.10	2.98*	1.90	1.30	4.31***
Criminal investigations	Employment	-1.48	-2.59**	-4.95***	11.01***	0.38	-5.39***
Criminal investigations	Citizen score	1.13	0.39	6.90***	6.29***	-1.56	8.80***
Healthcare	Banking	0.27	0.50	39.35***	5.35***	11.74***	-1.52
Healthcare	Crime prevention	1.30	1.48	38.70***	-8.14***	0.47	4.06***
Healthcare	Employment	-0.44	-1.20	29.74***	0.85	-0.34	-5.07***
Healthcare	Citizen score	2.41**	2.02**	44.31***	-4.63***	-2.19*	8.22***
Banking	Crime prevention	0.94	0.90	-1.36	-14.95***	-12.68***	6.13***
Banking	Employment	-0.63	-1.52	-9.26***	-4.74***	-12.81***	-3.89***
Banking	Citizen score	1.94	1.39	2.39*	-11.52***	-16.43***	10.88***
Crime prevention	Employment	-1.58	-2.39**	-8.11***	9.59***	-0.89	-9.88***
Crime prevention	Citizen score	0.96	0.48	3.92***	4.51***	-3.09**	4.44***
Employment	Citizen score	2.62**	2.89**	12.31***	-5.95***	-1.93	14.68***

Note: Similar direction of effect shows the number of domains per the total number of domains where the effect is significant and in the same direction. The remaining domains were not significant. Each column denotes factors and their levels. Below these, each row is a pairwise magnitude comparison showing z-scores using differences of the effect estimates found in different domains. To denote significance levels: $p < .05$, $**p < .01$, $***p < .001$.

presented with the outcomes (see supplemental materials) show that people were generally grateful for this technology and scored very low on negative emotional reactions.

4.2. Theoretical and practical implications

The present study used tools from the fields of moral psychology (Ditto et al., 2009) and decision-making (Samuelson & Zeckhauser, 1988) and combined them with privacy-related research (Acquisti et al., 2015) to contribute to the new domain of big data technologies. These technologies pose unique dilemmas and the conjoint design allowed us to pit factors against each other to simultaneously test which ones drive people’s evaluations. In most domains especially for evaluations of moral acceptability, people did not seem to be primarily driven by favorable outcomes but rather by data protection which challenges the notion that people only make decisions based on selfish motives. In most domains, people’s moral acceptability evaluations were driven by data protection thereby displaying risk or loss aversion (Harinck et al., 2012; Kahneman et al., 1991).

This was slightly different for the adoption of a technology. Data protection was the clear strongest driver in some domains (for example, banking) and outcome favorability was the clear strongest driver in another domain (for example, healthcare) which suggests that people’s decisions regarding privacy are malleable and change with context as argued by Acquisti et al. (2015). This could have direct implications for voting and referendums (Deutsch & Williams, 2017) about the implementation of these technologies. For example, in the criminal investigations domain, people were similarly driven by both factors of data protection and outcome favorability which could be a potential problem if a government policy favors one factor over the other. Additionally, a broad policy related to big data may not capture the

differences in people’s opinions across different domains and so policies would need to be different depending on what people prefer in a particular domain.

The results for the status quo factor are not in line with previous research that shows a general preference for the status quo (Samuelson & Zeckhauser, 1988) or existence bias (Eidelman et al., 2009), even if the new option may be more beneficial than the default (Suri et al., 2013). We ran additional analyses to check if age (instead of status quo) might have an effect on adoption. Age did seem to have a significant effect with older people more likely to adopt the technology. However, these effects were very small and must be interpreted carefully as the age range was restricted (most people were in the range [25, 45], very few people between ages 19–25, and 45–70). These results imply that in the context of big data technologies, in the presence of other factors like outcome favorability, data protection, and data sharing, status quo bias may not play a big role in evaluation of the technologies. The small preference of new technologies that are already in use elsewhere could imply that people may be more trusting of a technology if it is being used or accepted elsewhere.

4.3. Strengths and limitations

This study uses a design that has been shown to have high external validity (Hainmueller et al., 2015). However, it does have limitations. First, although we gave people an option to choose neither version of the technology, most people did not choose that option. It is difficult to say whether this choice was deliberate or whether seeing two versions of the technology directed people to choose a version more often than not choose a version at all. Thus, it is possible that actual levels of rejecting the technology may be higher than what we found in the study. If that is indeed the case, then it has implications for the results of the status quo

manipulation, which can only be observed in the differences in overall rejection rates across all of the different pairs of a technology.

Second, the manipulations of various levels of outcome favorability (e.g., favorable or unfavorable outcome) were not exactly the same in different domains (see Table 1). For example, in the healthcare domain, outcome favorability was about saving lives or not while in the banking domain, outcome favorability was about getting discounts or not. The manipulations necessarily varied with the domain which made it difficult to ensure that the factors would be manipulated to the same extent in different domains. They could have been strongly or weakly manipulated in some domains compared to others. We do think that this was a minor consequence of ensuring that the manipulations were as realistic as possible within each domain.

Third, we asked people to rate moral acceptability about technologies without measuring whether people found these technologies morally-relevant or not. For someone who does not see a technology as morally relevant, the question of moral acceptability may be hard to answer as there was no option to state that it was not applicable to the participant. That said, many of the issues surrounding big data are usually treated as moral in both literature (e.g., O'Neil, 2016) and in the media but it is not clear whether they are perceived as moral, and if so whether this view differs between people.

5. Conclusion

The rise of big data technologies and the costs and benefits that come with it make it important to understand how people evaluate these new technologies. We find that 1) outcome favorability and data protection drive these evaluations more than data sharing, with people placing equal or more importance on data protection in most domains; 2) there is no preference for the status quo except in the citizen scores domain; and 3) although all the technologies invade privacy to some extent, people still choose to accept the technology than reject it entirely when some of the factors are relevant to them. This research is a useful step in understanding the complex nature of big data technologies and how people place different levels of importance to different aspects of the technologies. Rather than testing factors independently, our approach considers factors simultaneously which provides a more realistic setting to study people's decision-making process when it comes to big data technologies.

Declaration of competing interest

None.

CRedit authorship contribution statement

Rabia I. Kodapanakkal: Conceptualization, Methodology, Formal analysis, Investigation, Writing - original draft. **Mark J. Brandt:** Conceptualization, Methodology, Writing - review & editing. **Christoph Kogler:** Conceptualization, Methodology, Writing - review & editing. **Ilja van Beest:** Conceptualization, Methodology, Writing - review & editing.

Acknowledgment

The second author received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 759320) for the drafting of this paper.

Appendix A. Supplementary data

Supplementary data to this article can be found online at <https://doi.org/10.1016/j.chb.2020.106303>.

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>.
- Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, 42(2), 249–274. <https://doi.org/10.1086/671754>.
- Bansak, K., Hainmueller, J., & Hangartner, D. (2016). How economic, humanitarian, and religious concerns shape European attitudes toward asylum seekers. *Science*, 309, 217–222. <https://doi.org/10.1126/science.aag2147>.
- Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, big data, and the public good frameworks for engagement* (pp. 44–75). Cambridge: Cambridge University Press.
- Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). *Revealed: Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian. <http://www.theguardian.com/>.
- Chopdar, P. K., Korfiatis, N., Sivakumar, V. J., & Lytras, M. D. (2018). Mobile shopping apps adoption and perceived risks: A cross-country perspective utilizing the unified theory of acceptance and use of technology. *Computers in Human Behavior*, 86, 109–128. <https://doi.org/10.1016/j.chb.2018.04.017>.
- Chuah, S. H.-W., Rauschnabel, P. A., Krey, N., Nguyen, B., Ramayah, T., & Lade, S. (2016). Wearable technologies: The role of usefulness and visibility in smartwatch adoption. *Computers in Human Behavior*, 65, 276–284. <https://doi.org/10.1016/j.chb.2016.07.047>.
- Church, M., Thambusamy, R., & Nemati, H. (2017). Privacy and pleasure: A paradox of the hedonic use of computer-mediated social networks. *Computers in Human Behavior*, 77, 121–131. <https://doi.org/10.1016/j.chb.2017.08.040>.
- Clegg, B. (2017). *Big data: How the information revolution is transforming our lives*. London: Icon Books Ltd.
- Coppock, A., Leeper, T. J., & Mullinix, K. J. (2018). Generalizability of heterogeneous treatment effect estimates across samples. *Proceedings of the National Academy of Sciences*, 115(49), 12441–12446. <https://doi.org/10.1073/pnas.1808083115>.
- Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, 10(1), 104–115. <https://doi.org/10.1287/orsc.10.1.104>.
- Dastin, J. (2018 October 10). Amazon scraps secret AI recruiting tool that showed bias against women. Reuters. <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scrap-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>.
- De Bekker-Grob, E. W., Donkers, B., Jonker, M. F., & Stolk, E. A. (2015). Sample size requirements for discrete-choice experiments in healthcare: A practical guide. *The Patient: Patient-Centered Outcomes Research*, 8(5), 373–384. <https://doi.org/10.1007/s40271-015-0118-z>.
- De Benedictis-Kessner, J., & Hankinson, M. (2019). Concentrated burdens: How self-interest and partisanship shape opinion on opioid treatment policy. *American Political Science Review*, 113(4), 1078–1084. <https://doi.org/10.1017/S0003055419000443>.
- Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83–108. <https://doi.org/10.1111/j.1083-6101.2009.01494.x>.
- Deutsch, A., & Williams, A. (2017, November). Netherlands to hold referendum on new surveillance law. Reuters. <http://uk.reuters.com/>.
- Ditto, P. H., Pizarro, D. A., & Tannenbaum, D. (2009). Motivated moral reasoning. *Psychology of Learning and Motivation*, 50, 307–338. [https://doi.org/10.1016/S0079-7421\(08\)00410-6](https://doi.org/10.1016/S0079-7421(08)00410-6).
- Dunn, J., Runge, R., & Snyder, M. (2018). Wearables and the medical revolution. *Personalized Medicine*, 15(5), 429–448. <https://doi.org/10.2217/pme-2018-0044>.
- Eidelman, S., Crandall, C. S., & Patterson, J. (2009). The existence bias. *Journal of Personality and Social Psychology*, 97(5), 765–775. <https://doi.org/10.1037/a0017058>.
- Epley, N., & Caruso, E. M. (2004). Egocentric ethics. *Social Justice Research*, 17(2), 171–187. <https://doi.org/10.1023/B:SORE.0000027408.72713.45>.
- Frondel, M., Simora, M., & Sommer, S. (2017). Risk perception of climate change: Empirical evidence for Germany. *Ecological Economics*, 137, 173–183. <https://doi.org/10.1016/j.ecolecon.2017.02.019>.
- Hainmueller, J., Hangartner, D., & Yamamoto, T. (2015). Validating vignette and conjoint survey experiments against real-world behavior. *Proceedings of the National Academy of Sciences*, 112(8), 2395–2400. <https://doi.org/10.1073/pnas.1416587112>.
- Hainmueller, J., Hopkins, D. J., & Yamamoto, T. (2013). Causal inference in conjoint analysis: Understanding multidimensional choices via stated preferences experiments. *Political Analysis*, 1–30. <https://doi.org/10.1093/pan/mpt024>.
- Harinck, F., Van Beest, I., Van Dijk, E., & Van Zeeland, M. (2012). Measurement-induced focusing and the magnitude of loss aversion: The difference between comparing gains to losses and losses to gains. *Judgment and Decision Making*, 7(4), 462–471.
- Johnson, E. J., & Goldstein, D. (2003). Do defaults save lives? *Science*, 302, 1338–1339. <https://doi.org/10.1126/science.109172>.
- Johnson, B. B., & Slovic, P. (1995). Presenting uncertainty in health risk assessment: Initial studies of its effects on risk perception and trust. *Risk Analysis*, 15(4), 485–494. <https://doi.org/10.1111/j.1539-6924.1995.tb00341.x>.
- Juma, C. (2016). *Innovation and its enemies: Why people resist new technologies*. New York, NY: Oxford University Press.

- Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). The endowment effect, loss aversion, and status quo bias. *The Journal of Economic Perspectives*, 5(1), 193–206. <https://doi.org/10.1257/jep.5.1.193>.
- Kleinberg, J., & Mullainathan, S. (2018). *Simplicity creates inequality: Implications for fairness, stereotypes, and interpretability*. arXiv preprint arXiv:1809.04578.
- Knudsen, E., & Johannesson, M. P. (2018). Beyond the limits of survey experiments: How conjoint designs advance causal inference in political communication research. *Political Communication*, 1–13. <https://doi.org/10.1080/10584609.2018.1493009>.
- Krehbiel, P. J., & Cropanzano, R. (2000). Procedural justice, outcome favorability, and emotion. *Social Justice Research*, 13(4), 339–360. <https://doi.org/10.1023/A:1007670909889>.
- Litman, L., Robinson, J., & Abbercock, T. (2017). TurkPrime.com: A versatile crowdsourcing data acquisition platform for the behavioral sciences. *Behavior Research Methods*, 49(2), 433–442. <https://doi.org/10.3758/s13428-016-0727-z>.
- Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, 1(2), 1–13. <https://doi.org/10.1177/2053951714541861>.
- Mahmood, K. (2019, July 12). *Three trends transforming stores into smart shopping hubs*. Forbes Technology Council. <https://www.forbes.com/sites/forbestechcouncil/2019/07/12/three-trends-transforming-stores-into-smart-shopping-hubs/#7aaa6d81602a>.
- Marr, B. (2019, January 21). Chinese social credit score: Utopian big data bliss or black mirror on steroids. Forbes. <https://www.forbes.com/sites/bemarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#d5e518548b83>. Retrieved from.
- McCandless, D., Evans, T., Barton, P., Tomasevic, S., & Geere, D. (2019, April 1). World's biggest data breaches and hacks. <https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>.
- Mims, C. (2019 August 3). When battlefield surveillance comes to your town. *The Wall Street Journal*. <https://www.wsj.com/articles/when-battlefield-surveillance-comes-to-your-town-11564805394>.
- Olsen, A. K., & Whalen, M. D. (2009). Public perceptions of the pharmaceutical industry and drug safety: Implications for the pharmacovigilance professional and the culture of safety. *Drug Safety*, 32(10), 805–810. <https://doi.org/10.2165/11316620-000000000-00000>.
- O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. New York, NY: Crown Publishing Group.
- Paharia, N., & Deshpande, R. (2009). Sweatshop labor is wrong unless the jeans are cute: Motivated moral disengagement. In *Harvard business school working paper* (pp. 9–79).
- Park, Y. J., & Shin, D. (2020). Contextualizing privacy on health-related use of information technology. *Computers in Human Behavior*, 105, 1–9. <https://doi.org/10.1016/j.chb.2019.106204>.
- Partala, T., & Saari, T. (2015). Understanding the most influential user experiences in successful and unsuccessful technology adoptions. *Computers in Human Behavior*, 53, 381–395. <https://doi.org/10.1016/j.chb.2015.07.012>.
- Pew Research Center. (2018, November 16). Public attitudes towards computer algorithms: Americans express broad concerns over the fairness and effectiveness of computer programs making important decisions in people's lives. <http://www.pewinternet.org/2018/11/16/public-attitudes-toward-computer-algorithms/>.
- Pew Research Center. (2019, July 22). Trust and distrust in America. <https://www.people-press.org/2019/07/22/trust-and-distrust-in-america/>.
- Potoglou, D., Dunkerley, F., Patil, S., & Robinson, N. (2017). Public preferences for internet surveillance, data retention and privacy enhancing services: Evidence from a pan-European study. *Computers in Human Behavior*, 75, 811–825. <https://doi.org/10.1016/j.chb.2017.06.007>.
- Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: Promise and potential. *Health Information Science and Systems*, 2(3), 1–10. <https://doi.org/10.1186/2047-2501-2-3>.
- Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty*, 1, 7–59. <https://doi.org/10.1007/BF00055564>.
- Spälti, A. K., Brandt, M. J., & Zeelenberg, M. Z. (2017). Memory retrieval processes help explain the incumbency advantage. *Judgment and Decision Making*, 12(2), 173–182.
- Stephens Davidowitz, S. (2017). *Everybody lies: Big data, new data, and what the internet can tell us about who we really are*. Dey Street Books.
- Strom, R. (2019 August 1). The algorithm will hire your patent lawyer now. Bloomberg Law. <https://biglawbusiness.com/the-algorithm-will-hire-your-patent-lawyer-now>.
- Suri, G., Sheppes, G., Schwartz, C., & Gross, J. J. (2013). Patient inertia and the status quo bias: When an inferior option is preferred. *Psychological Science*, 24(9), 1763–1769. <https://doi.org/10.1177/0956797613479976>.
- Tatonetti, N. P., Ye, P. P., Daneshjou, R., & Altman, R. B. (2012). Data-driven prediction of drug effects and interactions. *Science Translation Medicine*, 4(125), 125–131. <https://doi.org/10.1126/scitranslmed.3003377>.
- Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, 211, 453–458.
- Weeden, J., & Kurzban, R. (2017). Self-interest is often a major determinant of issue attitudes. *Political Psychology*, 38, 67–90. <https://doi.org/10.1111/pops.12392>.
- Williams, A. (2019, August 6). How to get access to the world's most exclusive wallet from metal Monzo to Amex Centurion cards. The Telegraph. <https://www.telegraph.co.uk/personal-banking/current-accounts/have-worlds-exclusive-wallet-metal-monzo-amex-centurion-cards/>.