This is an Accepted Manuscript for *Journal of Experimental Political Science* as part of the Cambridge Coronavirus Collection.
DOI: 10.1017/XPS.2020.30

Citizens' Attitudes to Contact Tracing Apps

Laszlo Horvath, Research Fellow, University of Exeter, Department of Politics
L.Horvath@exeter.ac.uk

Susan Banducci, Professor and Director of the Exeter Q-Step Centre, University of Exeter, Department of Politics

Oliver James, Professor of Political Science, University of Exeter, Department of Politics

Abstract:

Citizens' concerns about data privacy and data security breaches may reduce adoption of COVID-19 contact tracing mobile phone applications, making them less effective. We implement a choice experiment (conjoint experiment) where participants indicate which version of two contact tracing apps they would install, varying the apps' privacy-preserving attributes. Citizens do not always prioritize privacy and prefer a centralised National Health Service system over a decentralised system. In a further study asking about participants' preference for digital vs human-only contact tracing, we find a mixture of digital and human contact tracing is supported. We randomly allocated a subset of participants in each study to receive a stimulus priming data breach as a concern, before asking about contact tracing. Salient threat of unauthorised access or data theft does not significantly alter preferences in either study. We suggest COVID-19 and trust in a national public health service system mitigate respondents' concerns about privacy.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

Introduction[1]

Contact tracing mobile applications can help slow the spread of COVID-19 (Ferretti et al. 2020). However, citizens' concerns about data privacy and data security breaches may reduce adoption below the required coverage to be effective (Liu and Carter 2018; Ada Lovelace Institute 2020). We analyse the determinants of citizens' attitudes to these contact tracing apps. In *Study 1*, we implement a choice experiment (conjoint experiment) where participants indicated which version of two contact tracing apps they would be most likely to install. We vary the privacy-preserving attributes of the apps and estimate their effects on adoption. In *Study 2*, participants indicate preference for digital vs human-only contact tracing. To assess the salience of data breaches as an issue for adoption, we randomly allocated a subset of participants in each study to receive a stimulus priming data breach as a concern, before asking about contact tracing.

Under current pandemic conditions, we find that citizens do not always prioritize privacy but give high preference to a centralised system led by the National Health Service [NHS] over a decentralised system (see also Wiertz et al. 2020). Citizens tend to support a mixture of contact tracing done digitally with limited human involvement. Salient threat of unauthorised access or data theft does not significantly alter either set of preferences.

[1] Support for this research was provided by the Economic and Social Research Council (Award No. ES/R005133/1), the Exeter Q-Step Centre and the College of Social Sciences and International Studies at the University of Exeter. Susan Banducci's work was supported through a Turing Fellowship, The Alan Turing Institute, UK. The authors declare no conflicts of interest. The data, code, and any additional materials required to replicate all analyses in this article are available at the Journal of Experimental Political Science Dataverse within the Harvard Dataverse Network, at: doi:10.7910/DVN/KVKGUB.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

Theory and hypotheses

Research on the adoption of technology similar to mobile phone contact tracing applications has shown that users' concern about data security and privacy can reduce acceptance. A study of predictors of individuals' adoption of healthcare wearable devices found that individuals' privacy perceptions were an important part of their calculations about use of the technology (Li et al. 2016). This leads to our first hypothesis:

> **Baseline preference of privacy.** We hypothesise a baseline preference of more privacy-preserving contact tracing applications.

The process of contact tracing using apps in practice supplements traditional human contract tracing. There is little direct evidence about this issue for COVID-19 but the broader literature on algorithm aversion suggests that people tend to prefer human involvement in systems even if they perform less well (Dietvorst 2015). We therefore propose the following hypothesis:

> **Baseline preference of human contact tracing.** We hypothesise that citizens prefer more human involvement over digital-only contact tracing.

The concerns of users about privacy and preference for human contact tracing lead us to further examine whether making the possibility of data breaches more salient strengthens these baseline preferences, leading to a third hypothesis:

> **Saliency of data breach.** We hypothesise that preferences of privacy preserving contact tracing, as well as human contact tracing, are strengthened for individuals who consider data breach as a realistic threat.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

The international experience with COVID-19 has shown that citizens' responses and willingness to engage with public health measures are affected by broader socio-political attitudes. Recently, evidence has emerged about differences based on partisanship (e.g. Utych 2020) and gender (Palmer and Peterson 2020). In the UK context, where our studies are based, there is less clear evidence about partisan divides but the issue of other political attitudes towards the public authorities proposing the use of technology is still salient. Previous studies have found that trust in organisations is a factor influencing intention to use related digital government technologies (van Velsen et al. 2015). For these reasons, we include measures of trust in the National Health Service, and trust in the UK government's handling of COVID-19. In each case, higher trust is expected to increase acceptance of privacy reducing and more technology reliant aspects of the mobile phone app.

Globally, digital contact tracing is being rolled out with a variety of system architectures that have different implications for privacy and data security. The core functionalities of a *centralised system* are performed by a central server processing user data, which is managed by a health authority and can, subject to permissions, notify an infected user's contacts of exposure (Ahmed et al. 2020, 134578-134580; Martin et al. 2020). A *decentralised system*, on the other hand, has most of its core functionalities performed by users' devices including exposure notifications (Ahmed et al. 2020, 134580-134581). The privacy implications of these two systems have often been discussed as a trade-off with other attributes (see also Cioroianu and Dal 2020 for an overview). While decentralised systems are recommended for

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

having more overall privacy-preserving features than centralised systems[2], the lack of central oversight does limit human involvement in the process of contact tracing. This might be problematic while contact tracing apps tend to perform with poor accuracy (Briers 2020). By contrast, whereas centralised systems do have the ability to integrate digital with human contact tracing and research (by design, but in practice may be a legislative feature), their data servers are vulnerable to data breach that involves more sensitive protected data.

Methods

Subjects and context[3]

Study 1, uses an online panel of N = 1,504 from Dynata, targeting a diversity of respondents representative of the UK as of its 2011 census[4], *Study 2*, uses a smaller, N = 809 panel from Prolific Academic, with similar sample demographics[5,6]. Data collection occurred 18 May

[2] A central data server is especially vulnerable to a single point of failure (Ahmed et al. 2020, 134585) but as Baumgärtner et al (2020) show, decentralised systems are vulnerable to potential profiling of individual user locations.

[3] The research design presented here was reviewed and approved by the University of Exeter College of Social Sciences and International Studies Ethics Committee, and pre-registered at Aspredicted.org Study No. #41234 prior to data collection.

[4] Our target sample size for Study 1 was 1,500 to allow us for a minimum detectable effect size of approximately 5% on a four-level attribute across five discrete choice tasks.

[5] Study 2 requires substantially fewer observations based on power considerations only. We targeted 800 towards the lower end N where the data provider offered the option of representative demographics.

[6] Distribution of age, gender, and region of residence are summarised in Appendix A. Other than compliance with our demographic quotas (managed by the data supplier) and indication

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

2020 to 23 May 2020. During this period, the UK had no official (government-backed) contact tracing app available for public use, except for a trial version released on the Isle of Wight exclusively. That application was one of the centralised systems as outlined above. The UK's next contact tracing app to enter a new trial phase will be built on a decentralised system (Department of Health & Social Care 2020).

Dependent measures

In the *Study 1 conjoint experiment*, respondents were asked to choose one of two COVID-19 contact tracing apps to install, with their data privacy and security attributes varying. Each respondent made a series of five such selections.

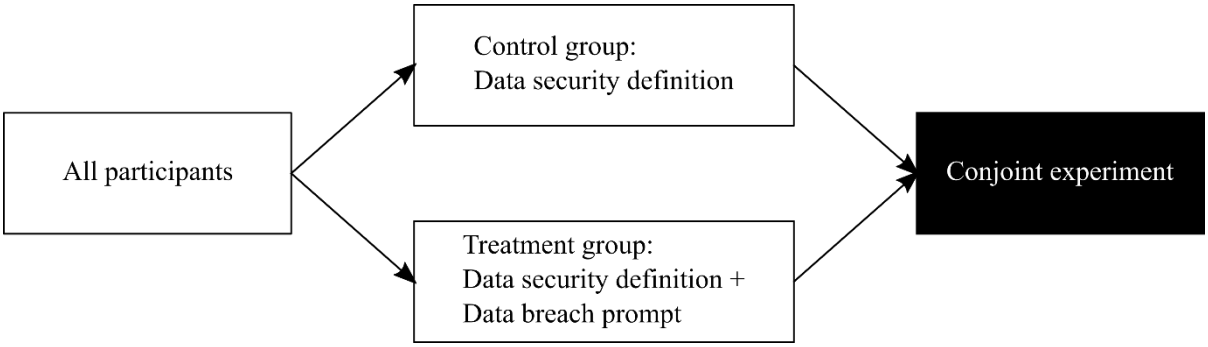


Fig. 1: Overview of Study 1

In *Study 2*, the dependent measure is respondents' preferred amount of human involvement in the process of COVID-19 contact tracing. This is a rating scale ranging from human-only contact tracing (1) to digital only contact tracing (7).

---

of informed consent, there were no additional inclusion criteria to participate and paid respondents self-selected to participate.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

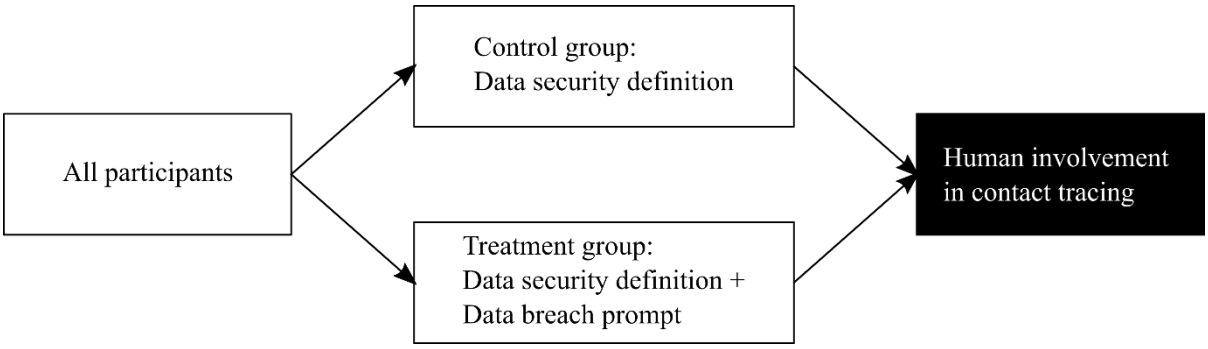


Fig. 2: Overview of Study 2

Treatment: Data breach stimulus

Both groups in each Study received a brief text about data security including its definition as "a set of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure." The treatment group additionally got text about data breaches becoming "more common," giving examples: "theft of personal data, devices containing personal data being lost or stolen[7]."

Conjoint experiment

The conjoint experiment enabled us to assess the causal impact of multiple attributes related to privacy and data security: *data storage, until when data is stored, what kinds of contacts and what specificity of location is uploaded, and what constitutes a contact*.

[7] We examine compliance with treatment in Appendix B.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

Conventional conjoint experiments randomise and display all attributes independently. Our challenge, however, was to capture two vastly different implementations of digital contact tracing with their privacy options fundamentally incompatible with each other, restricting the option of independent randomisation. Decentralised systems of digital contact tracing use minimal data sharing across devices whereas centralised systems use data sharing between devices and a data server. As explained above, decentralised systems may preserve privacy better but are not integrated with human contact tracing and research in contrast to centralised systems that can be integrated but may consequently be seen as vulnerable to data breaches.

We address the issue using *dependent attributes*. Respondents evaluate five pairs of potential contact tracing applications that compare either a decentralised system that simply does not store contact or location data with a centralised system that stores at least one of these, or two centralised systems with varying privacy attributes excluding the possibility of no data storage. In this way, attributes presented in Table 1 below are heavily system-dependent.

As attributes are not fully independent we (1) present a comparison of effect sizes on the data storage attribute alone, independently from the privacy attributes, and then (2) present the effect of the rest of the privacy attributes separately on respondents who compared two centralised systems[8].

[8] We include more explanation in Appendix B.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

Table 1: Privacy attributes depending on data storage system (dependent attributes)

Data storage

Decentralised, locally on device	In a central database: NHS	In a central database: Gov't

Purpose of app (explanatory attribute only)

Notify user directly of exposure	Inform human contact tracer to examine user's exposure to virus

Data stored until

Not stored	Indefinitely	Tests widely available	Vaccine available

Location uploaded

None	Exact location	1st part of postcode area

Contacts uploaded

None	All contacts	Person with symptoms

What constitutes a contact

6ft / 5mins	6ft / 15mins	12ft / 5mins	12ft / 15mins

Note: A third of all binary comparisons were between a centralised system (privacy attributes varying) and a decentralised system (privacy attributes not varying), and two-thirds between two centralised systems (privacy attributes varying, greyed cells). Privacy-varying attributes reported on latter subsample.

Moderators

We include the following as moderators of conjoint preferences: trust in the National Health Service and satisfaction with the government's handling of coronavirus[9].

[9] "Please tell me on a scale of 0-10 how much you personally trust the National Health Service [NHS] where 0 means you do not trust the NHS at all, and 10 means you have complete trust," and "How well or badly do you think the UK government is handling the coronavirus (Covid-19) outbreak?" expressed on a 1 (Very badly) to 4 (Very well) scale.

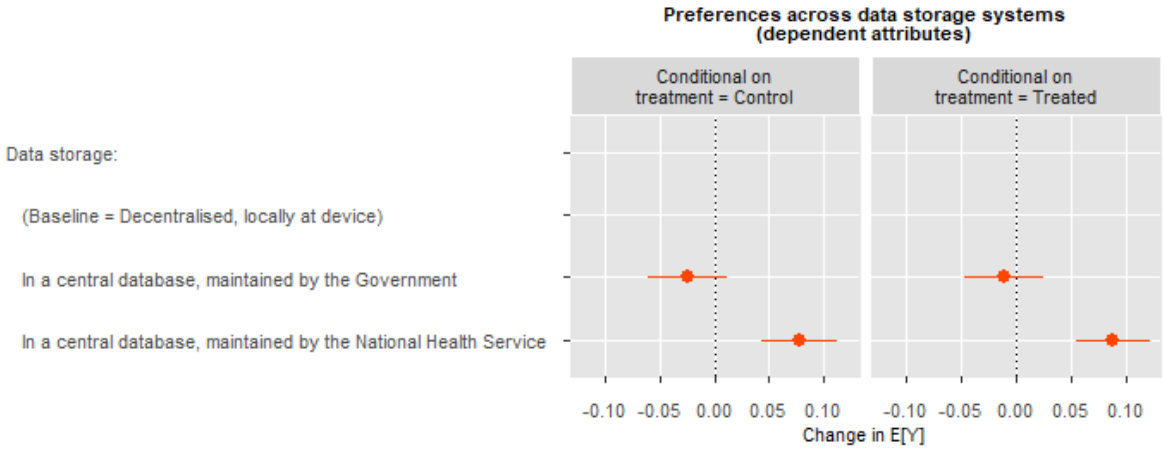
Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

Results

Study 1

Descriptive results. Across all attributes, respondents do not systematically prefer more privacy. For data storage, the NHS led centralised system is preferred in 55.94% of binary comparisons compared to the centralised system led by the UK government (45.85%) and the decentralised system (47.63%) despite the NHS system being potentially displayed with attributes more intrusive to privacy.[10]

Treatment effects: Data storage. In the pooled model across all conjoint choices (five tasks, two profiles per task displayed by respondents thus N = 15,040) with standard errors clustered on the respondent level, we found no difference between preference for data storage and exposure to the data breach stimuli.



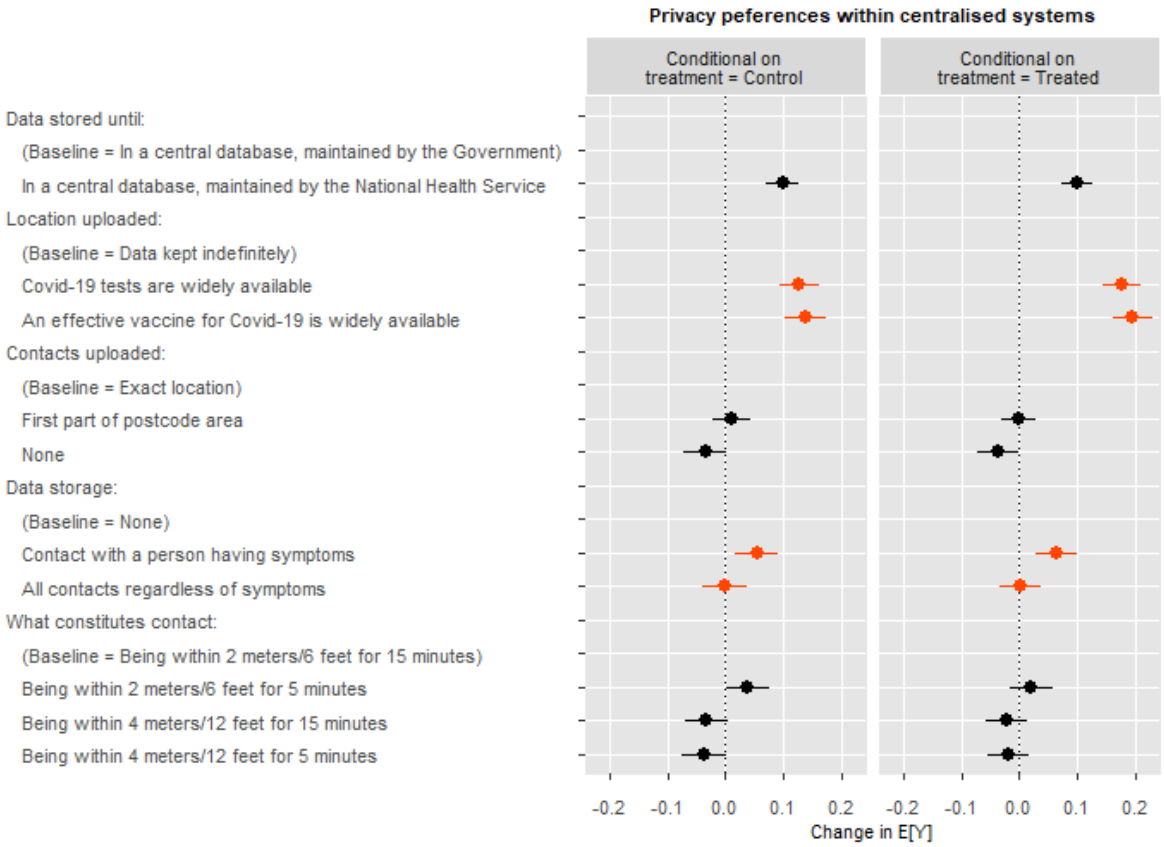
Note: Treatment is exposure to stimulus raising awareness of data breach. AMCE values calculated with the cjoint (Hainmueller et al. 2014) package in R. For ATE values (coefficients) see Table 2.

Fig. 3: Treatment effects on preference of data storage systems

[10] We show the obtained distribution of all conjoint preferences in Appendix C.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

Treatment effects within centralised data storage systems. An N = 10,950 app profiles described a centralised system with further attributes relating to privacy varying. In this subset of the data, our model finds no treatment effects relating to exposure to the data breach stimulus except some evidence that the stimulus may have further strengthened respondents' preference to store data until vaccines or tests are available over indefinite data storage.



Note: Treatment is exposure to stimulus raising awareness of data breach. AMCE values calculated with the cjoint (Hainmueller et al. 2014) package in R. For ATE values (coefficients) see Table 3.

Fig. 4: Treatment effects on privacy preferences within centralised systems

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

Trust in NHS as a moderator. In two similar pooled models as above, across data storage systems as well as within centralised systems we find that although high trust in the NHS strengthens preferences for an NHS-led centralised system, low trust in the NHS does not mean clear support for a decentralised system (or a centralised one maintained by the government). Within centralised systems, trust in the NHS motivates respondents to give up more privacy.

Government performance as moderator. Satisfaction with the government's performance in handling COVID-19 moderated preferences given to a centralised system maintained by the UK government. Across the spectrum, however, the NHS-led centralised system remains the clear preference in the majority of comparisons.

Table 2: Data storage models

	Treatment	**Moderator 1:** NHS trust	**Moderator 2:** Gov't performance
Dependent variable: Pr(profile chosen)			
Intercept (Baseline: Decentralised, stored on device)	-0.08	0.31*	0.18*
	(0.05)	(0.15)	(0.09)
Covariate (see notes)	-0.04	-0.05**	-0.11**
	(0.06)	(0.02)	(0.03)
In a central database, maintained by the government	-0.10	-0.35	-0.72***
	(0.06)	(0.20)	(0.12)
In a central database, maintained by the National Health Service	0.31***	-0.49*	0.24
	(0.06)	(0.20)	(0.12)
Covariate x In a central database, maintained by the government	0.05	0.03	0.25***
	(0.08)	(0.02)	(0.04)
Covariate x In a central database, maintained by the National Health Service	0.04	0.10***	0.04
	(0.08)	(0.02)	(0.04)
AIC	20737.13	20718.81	20356.22
Log Likelihood	-10362.57	-10353.41	-10172.11
Num. obs.	15040	15040	14790

***p < 0.001, **p < 0.01, *p < 0.05.
Pooled GLM estimates with standard errors clustered on respondent level.
Note: For simplified display, "Covariate" means "Treatment" in the first, "Trust in NHS" in the second, and "Gov't performance" in the third column.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

Table 3: Treatment and moderator effects on preference within centralised systems

	Treatment	**Moderator 1:** NHS trust	**Moderator 2:** Gov't performance
Dependent variable: Pr(profile chosen)			
Intercept	-0.57***	-0.82*	-1.21***
	(0.09)	(0.32)	(0.20)
Covariate (see notes)	-0.15	0.02	0.22**
	(0.13)	(0.04)	(0.07)
In a central database, maintained by the National Health Service	0.41***	-0.12	0.98***
	(0.06)	(0.19)	(0.12)
Covid-19 tests are widely available	0.52***	0.16	0.79***
	(0.07)	(0.23)	(0.14)
An effective vaccine for Covid-19 is widely available	0.56***	0.46	0.96***
	(0.07)	(0.23)	(0.15)
First part of postcode area	0.04	0.27	-0.10
	(0.06)	(0.22)	(0.14)
None	-0.14	0.68**	-0.07
	(0.08)	(0.26)	(0.16)
Contact with person having symptoms	0.23**	0.44	0.31*
	(0.08)	(0.25)	(0.16)
All contacts regardless of symptoms	-0.00	-0.08	0.01
	(0.08)	(0.26)	(0.16)
Within 2 meters/6 feet for 5 minutes	0.16*	0.26	0.29
	(0.08)	(0.27)	(0.17)
Within 4 meters/12 feet for 15 minutes	-0.13	0.14	-0.14
	(0.08)	(0.26)	(0.17)
Within 4 meters/12 feet for 5 minutes	-0.15	0.23	-0.13
	(0.08)	(0.27)	(0.17)
Covariate x In a central database,	0.01	0.06**	-0.22***

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

maintained by the National Health Service	(0.08)	(0.02)	(0.04)
Covariate x Covid-19 tests are widely available	0.21*	0.06*	-0.06
	(0.10)	(0.03)	(0.05)
Covariate x An effective vaccine for Covid-19 is widely available	0.24*	0.03	-0.10
	(0.10)	(0.03)	(0.05)
Covariate x First part of postcode area	-0.05	-0.03	0.04
	(0.09)	(0.03)	(0.05)
Covariate x None	-0.01	-0.10**	-0.03
	(0.11)	(0.03)	(0.06)
Covariate x Contact with person having symptoms	0.04	-0.02	-0.02
	(0.11)	(0.03)	(0.06)
Covariate x All contacts regardless of symptoms	0.01	0.01	-0.01
	(0.11)	(0.03)	(0.06)
Covariate x Within 2 meters/6 feet for 5 minutes	-0.07	-0.02	-0.07
	(0.11)	(0.03)	(0.06)
Covariate x Within 4 meters/12 feet for 15 minutes	0.04	-0.03	0.01
	(0.11)	(0.03)	(0.06)
Covariate x Within 4 meters/12 feet for 5 minutes	0.07	-0.04	0.00
	(0.11)	(0.03)	(0.06)
AIC	14776.57	14756.40	14494.44
Log Likelihood	-7366.29	-7356.20	-7225.22
Num. obs.	10950	10950	10766

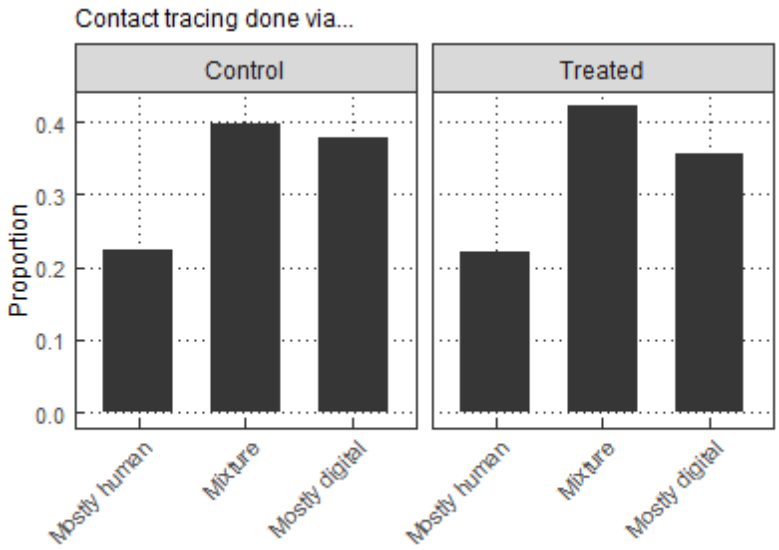
*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$
Pooled GLM estimates with standard errors clustered on respondent level.
Note: For simplified display, "Covariate" means "Treatment" in the first, "Trust in NHS" in the second, and "Gov't performance" in the third column.

Study 2

Study 2 repeated the data breach stimulus asking respondents about their preferred amount of human involvement in the process of contact tracing. The majority of citizens prefer a

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

mixture between human-led and digital, with greater proportions preferring "Mostly digital" to "Mostly human"[11]. We find no significant treatment effects for exposure to data breaches.



Note: Treatment is exposure to stimulus raising awareness of data breach.

Fig. 5: Preference of digital vs human contact tracing per treatment group

[11] We show the original distribution of preferences descriptively in Appendix C.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

Table 4: Treatment effects on preferred amount of human involvement in contact tracing

	Pr(*y* = **Mostly human**)	Pr(*y* = **Mixture**)	Pr(*y* = **Mostly digital**)
Intercept	-1.24***	-0.42***	-0.50***
	(0.12)	(0.10)	(0.10)
Treated	-0.01	0.10	-0.09
	(0.17)	(0.14)	(0.15)
AIC	864.11	1098.15	1067.26
Log Likelihood	-430.05	-547.07	-531.63
Num. obs.	809	809	809

*** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$

Discussion and conclusions

Citizens prefer a balanced (human plus digital) approach to contract tracing. Privacy concerns were not as influential on choice of the digital app as initially expected and as indicated by past research. Privacy concerns were overridden by trust in the NHS and the NHS centralised app is preferred to both the centralised government app and the decentralised system. The NHS has strong support amongst the UK public; support and research on other public services has found users have greater willingness to cooperate in the coproduction of public services delivered by public organisations when compared to services delivered under contract to private companies (James and Jilke 2020). Our findings are consistent with this line of research and demonstrate that when a trusted public health provider is involved in the development and deployment of the tracing app it can bring about the cooperation of the public necessary for its successful use in reducing the spread of infection.

Our results suggest two considerations for future research. First, to further understand the role of health care providers, research should examine the effect of institutional differences on coproduction, including whether the organisation is public or privately owned. The unique status of the NHS with its current high regard among the British public may not

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

translate to coproduction in all other jurisdictions. Second, variation in the perceptions of the salience of the COVID-19 threat across different countries and populations might explain how the public responds to privacy concerns. The data breach treatment does not influence outcomes, possibly because of crisis perceptions which were likely high in the initial phase of the pandemic. Potential changes in responses over time as the pandemic develops and differences in findings between jurisdictions with different public health systems are particularly important topics for future research.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

References

Ada Lovelace Institute. (2020). COVID-19 Rapid Evidence Review: Exit through the App Store? https://www.adalovelaceinstitute.org/exit-through-the-app-store-how-the-uk-government-should-use-technology-to-transition-from-the-covid-19-global-public-health-crisis/

Ahmed, N., Michelin, R. A., Xue, W., Ruj, S., Malaney, R., Kanhere, S. S., ... & Jha, S. (2020). A survey of covid-19 contact tracing apps. *IEEE Access*, 134577-134601 DOI: 10.1109/ACCESS.2020.3010226

Baumgärtner, L., Dmitrienko, A., Freisleben, B., Gruler, A., Höchst, J., Kühlberg, J., ... & Penning, A. (2020). Mind the GAP: Security & Privacy Risks of Contact Tracing Apps. arXiv preprint arXiv:2006.05914.

Briers, M. (2020). A technical roadmap for the UK's contact tracing app functionality. The Alan Turing Institute Blog, https://www.turing.ac.uk/blog/technical-roadmap-uks-contract-tracing-app-functionality

Cioroianu, I., Dal, A. (2020). What is missing from the online debate around COVID-19 digital tools? Institute of Policy Research Blog, University of Bath, https://blogs.bath.ac.uk/iprblog/2020/07/08/what-is-missing-from-the-online-debate-around-covid-19-digital-tools/

Department of Health and Social Care. (2020). The NHS Test and Trace App (early adopter trial, August 2020): data protection impact assessment, Published 13 August 2020, https://www.gov.uk/government/publications/nhs-test-and-trace-app-privacy-information/the-nhs-test-and-trace-app-early-adopter-trial-august-2020-data-protection-impact-assessment

Dietvorst, B., Simmons, J. P., & Massey, C. (2015). Algorithm Aversion: People Erroneously Avoid Algorithms after Seeing Them Err. *Journal of Experimental Psychology: General*, 144 (1), 114-126, DOI: 10.1037/xge0000033

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., Parker, M., Bonsall, D., & Fraser, C. (2020). Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing. *Science, 368*(6491), DOI: 10.1126/science.abb6936

Hainmueller, J., Hopkins, D., and Yamamoto T. (2014). Causal Inference in Conjoint Analysis: Understanding Multi-Dimensional Choices via Stated Preference Experiments. *Political Analysis* 22(1):1-30, DOI: 10.1093/pan/mpt024

Horvath, L., Banducci, S., James, O. (2020). Replication Data for: Citizens' Attitudes to Contact Tracing Apps. Harvard Dataverse, DOI: 10.7910/DVN/KVKGUB

James, O., and Jilke, S. (2020). Marketisation Reforms and Coproduction: Does Ownership of Service Delivery Structures and Customer Language Matter?. Public Administration https://doi.org/10.1111/padm.12670

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

Li, H., Wu, J., Gao, Y., & Shi, Y. (2016). Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective. *International Journal of Medical Informatics*, 88, 8-17.

Liu, D. and Carter, L. (2018). Impact of Citizens' Privacy Concerns on e-Government Adoption. In *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 1-6, DOI: 10.1145/3209281.3209340

Martin, T., Karopoulos, G., Hernández-Ramos, J. L., Kambourakis, G., & Fovino, I. N. (2020). Demystifying COVID-19 digital contact tracing: A survey on frameworks and mobile apps. arXiv preprint, arXiv:2007.11687.

Palmer, C. L., & Peterson, R. D. (2020) Toxic Mask-ulinity: The link between masculine toughness and affective reactions to mask wearing in the COVID-19 era. *Politics & Gender*, 1-14, DOI: 10.1017/S1743923X20000422P

Utych, S. M. (2020) Messaging mask wearing during the COVID-19 crisis: Ideological differences. *Journal of Experimental Political Science*, 1-15, DOI: 10.1017/XPS.2020.15

van Velsen, L., van der Geest, T., van de Wijngaert, L., van den Berg, S., Steehouder, M. (2015). Personalization Has a Price, Controllability is the Currency: Predictors for the Intention to Use Personalized eGovernment Websites. *Journal of Organizational Computing and Electronic Commerce, 25(1)*, 76-97, DOI: 10.1080/10919392.2015.990782

Wiertz, C., Banerjee, A., Acar, O. A., Ghosh, A. (2020). Predicted Adoption Rates of Contact Tracing App Configurations---Insights from a Choice-Based Conjoint Study with a Representative Sample of the UK population. SSRN Preprint, DOI: 10.2139/ssrn.3589199

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

Appendix A: Sample characteristics

Sample demographics

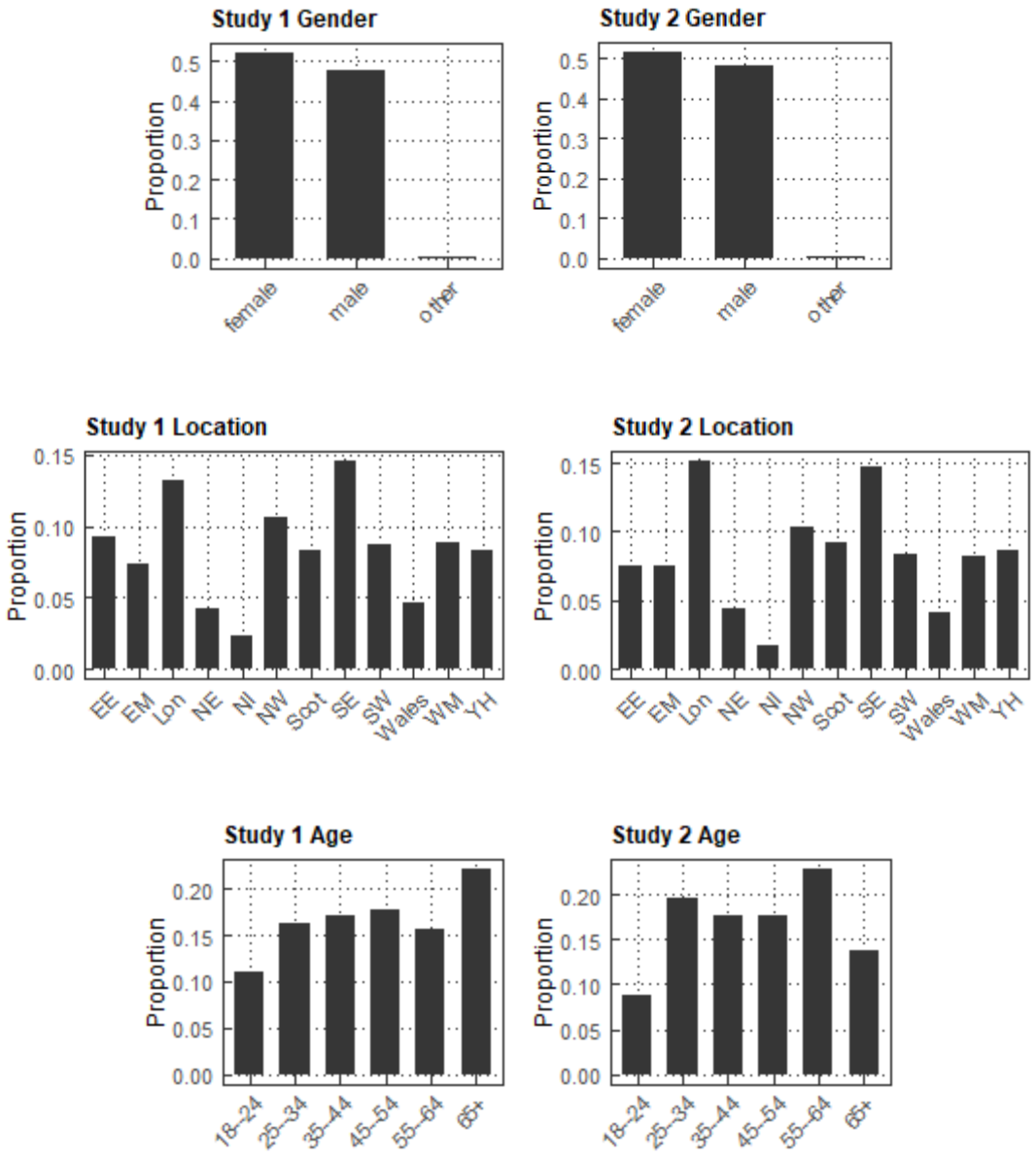


Fig. A1: Distribution of key sample demographics

Attention checks

Adapted from Berinsky et al. 2014:

1. In a block of four questions relating to gender discrimination, statement No. 4 read "Please click the "neither agree nor disagree" response to continue with survey." The ratio of incorrect responses to the total number of responses is 11.77%.
2. In a block of four questions relating to attitudes to UK government policy, statement No. 4 read "Two is greater than one." The ratio of incorrect responses to the total number of responses is 19.74%.

The distribution of conjoint preferences as well as treatment effects are robust to data quality. On the subsample of respondents who passed both checks, N = 1,095:

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

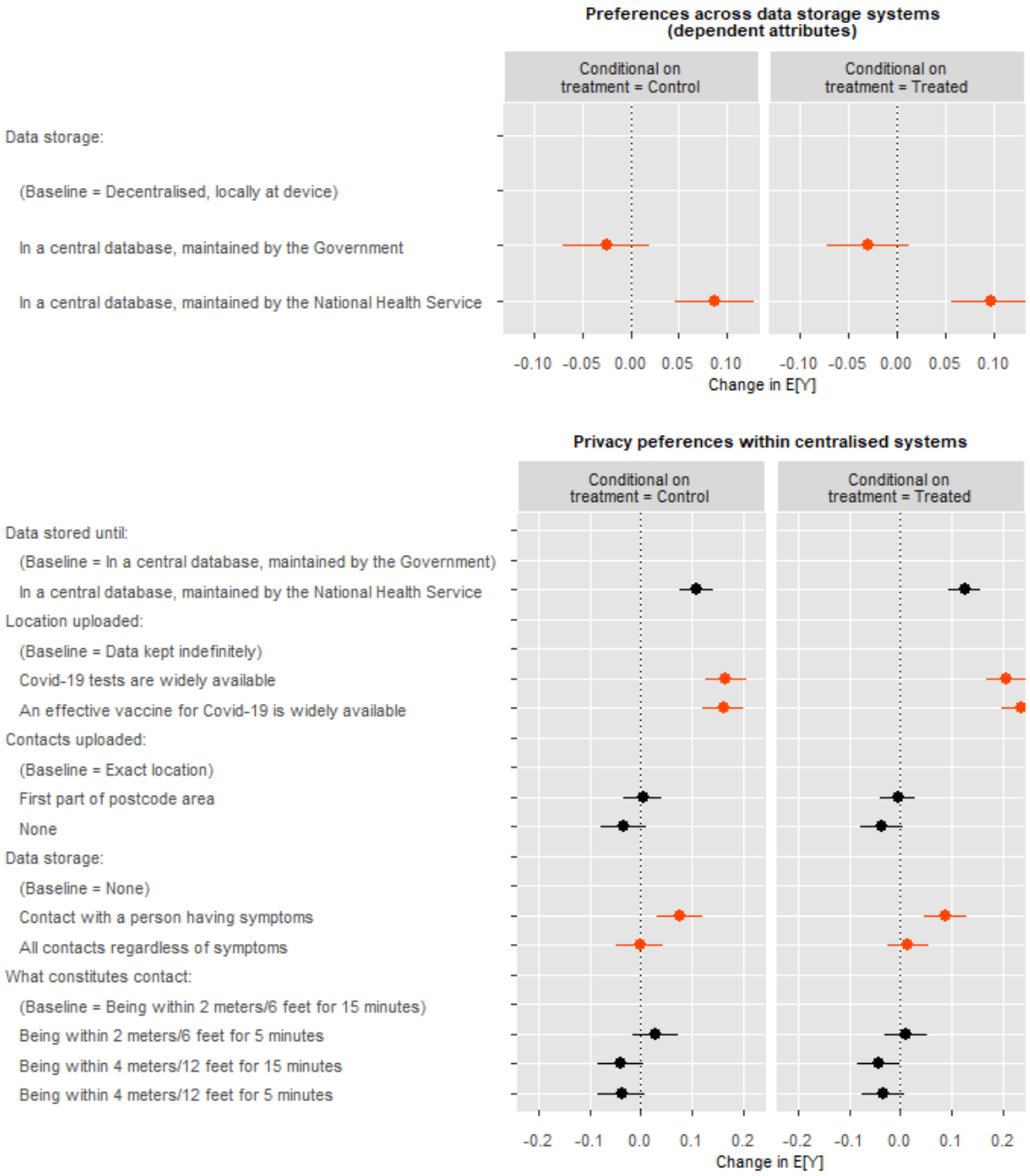


Fig. A2: Conjoint preferences among those who passed both attention checks

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

Appendix B: Treatment details

Stimulus wording

Table B1: Data breach stimulus wording

Control group	Treatment
Data security is a set of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure. Data security can be applied using a range of techniques and technologies, including administrative controls, physical security, and other safeguarding techniques that limit access to unauthorized or malicious users or processes.	Data security is a set of standards and technologies that protect data from intentional or accidental destruction, modification or disclosure. Data security can be applied using a range of techniques and technologies, including administrative controls, physical security, and other safeguarding techniques that limit access to unauthorized or malicious users or processes. Data breaches, however, are becoming more common. For example, data breaches could include hackers getting unauthorised access to or theft of personal data, devices containing personal data being lost or stolen.

Compliance with treatment

This stimulus was not pre-tested. To scrutinise compliance with treatment, after the dependent measures, we checked respondent recall of the four terms listed (see Appendix B). Respondents in the treatment group were over two and a half times more likely to recall the term "theft of personal data" than respondents in the control group among other terms, $\chi^2(1, 1504) = 53.4$, $p < 0.01$. In Study 2, respondents in the treatment group were nearly seven times more likely to recall the this term, $\chi^2(1, 809) = 83.1$, $p < 0.01$

Randomisation result

Randomisation was successful: In Study 1 and Study 2, 52.13% and 51.66% of respondents were assigned into the data breaches group, respectively.

Display frequency of conjoint attributes

We used the Conjoint Survey Design Tool (SDT, Strezhnev et al. 2014) to program this experiment. The PHP script generating the app profiles may be viewed at the web address http://qsteplin.ex.ac.uk/conjoint/ctrace.php.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

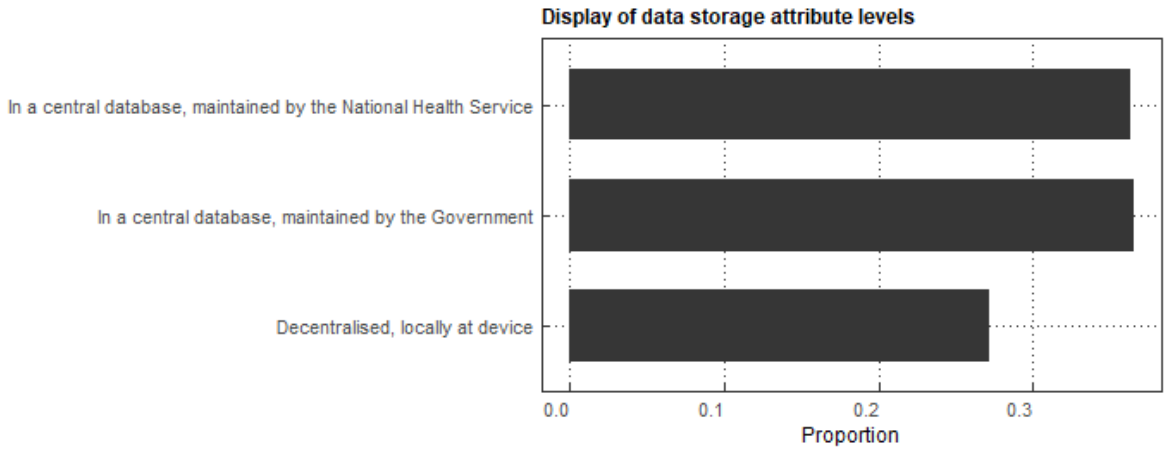


Fig. B1: Display frequency of data storage attribute

The various privacy attributes displayed in the app profiles depended on them being "central database" systems. We explain this reasoning behind this in Section Methods. While we note that attribute constraints are to be used sparingly in conjoint analysis (Strezhnev et al. 2014) we used this constraint to reflect the real-life choice citizens may face between a possible privacy preserving app (Troncoso et al. 2020) and a centralised system that collects protected personal data (Veale 2020). Our system-dependent attributes were resolved by the CDT program by displaying decentralised systems with somewhat lower frequency (by 9.09%). To avoid biased randomisation inference due to dependency of privacy attributes, they were only analysed on the subsample of tasks that did not involve a decentralised system---however, the results do not change significantly looking at the distribution of conjoint preferences descriptively on the full sample, see Appendix C.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

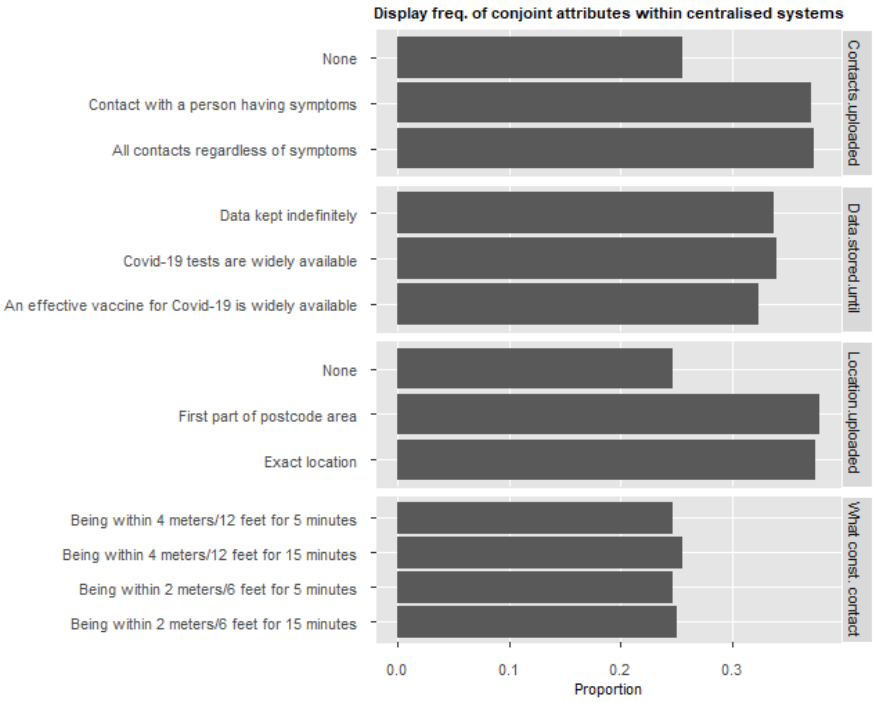


Fig. B2: Display frequency of privacy attributes within centralised systems

The distribution of privacy attributes is impacted by a single constraint we introduced: as centralised systems collect personal data, could not allow that "Contacts uploaded" as well as "Location uploaded" to be displayed "None" at the same time. We did however allow No Location data to be collected if some Contact data was collected and vice versa.

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30

Appendix C: Observed distribution of dependent measures

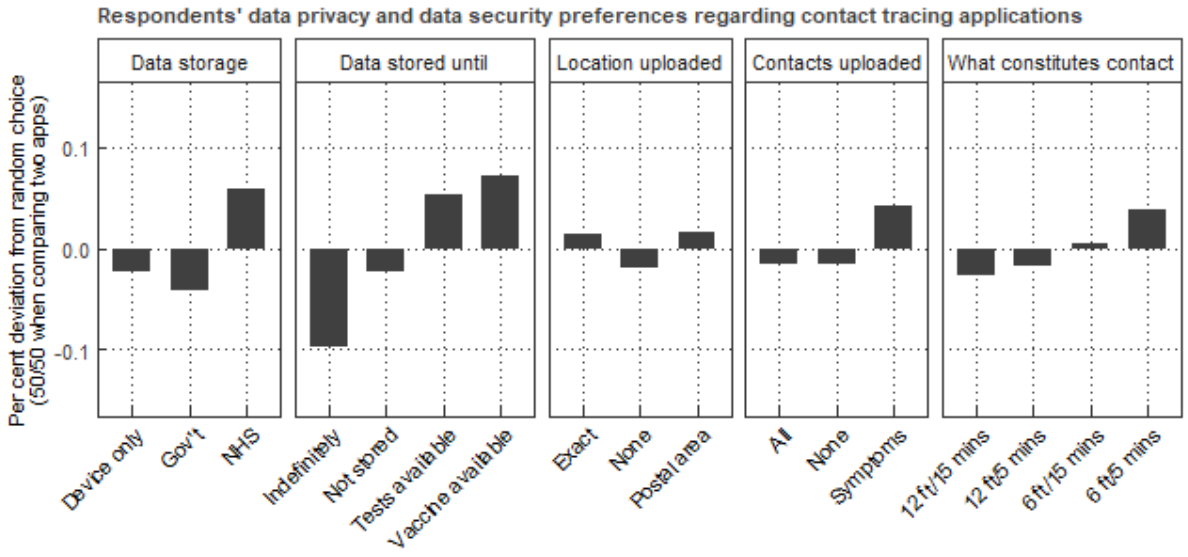


Fig. C1: Overview of app choice by conjoint attributes

Fig. C2: Observed app choice by data breaches treatment group

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

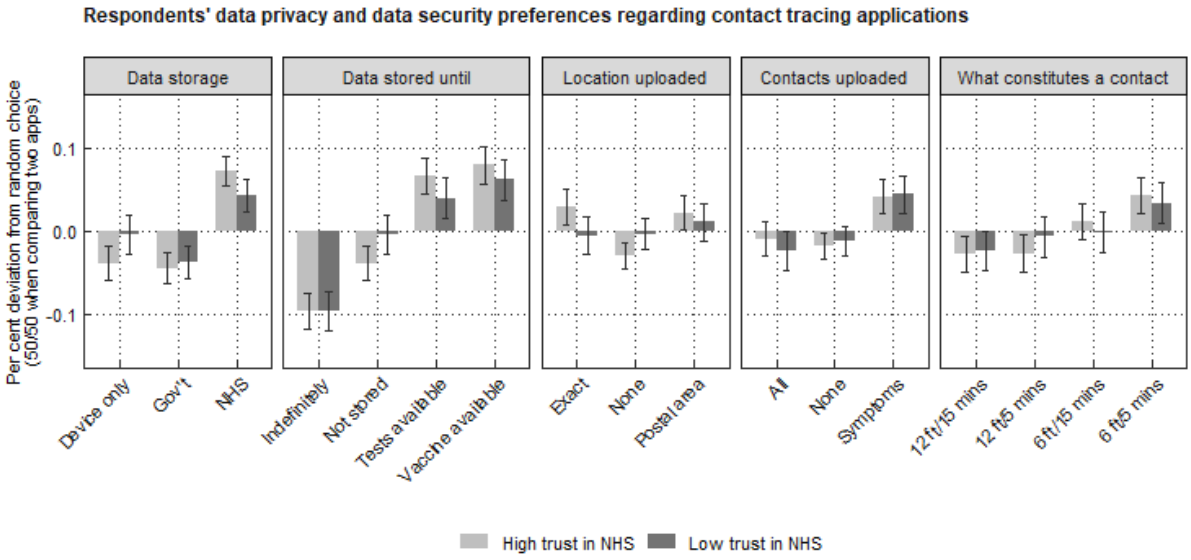


Fig. C3: Observed app choice by moderator 1: trust in NHS

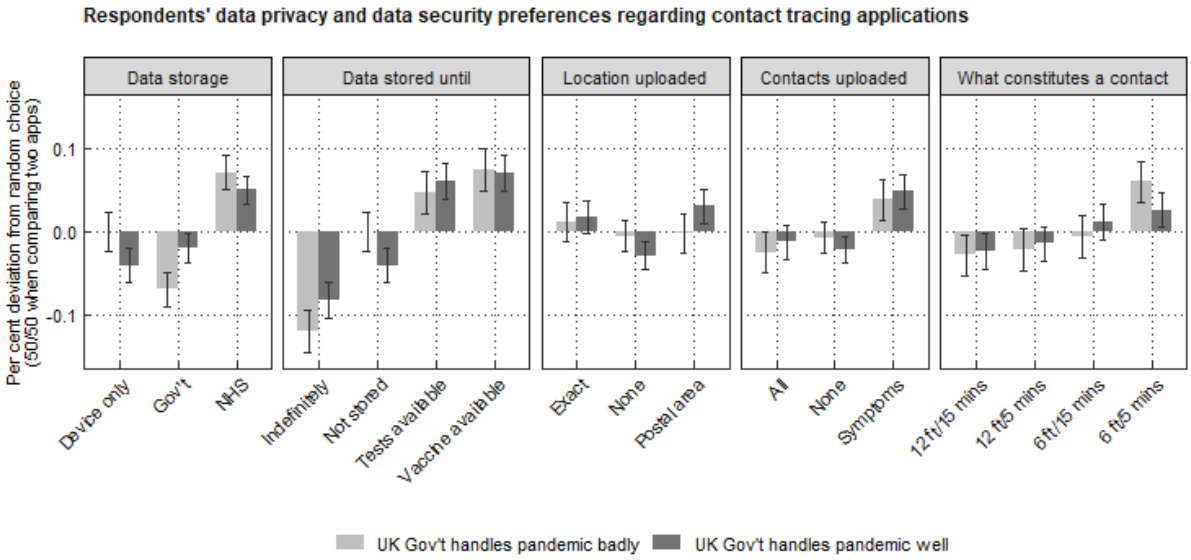


Fig. C4: Observed app choice by moderator 1: Government performance

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms.
https://doi.org/10.1017/XPS.2020.30

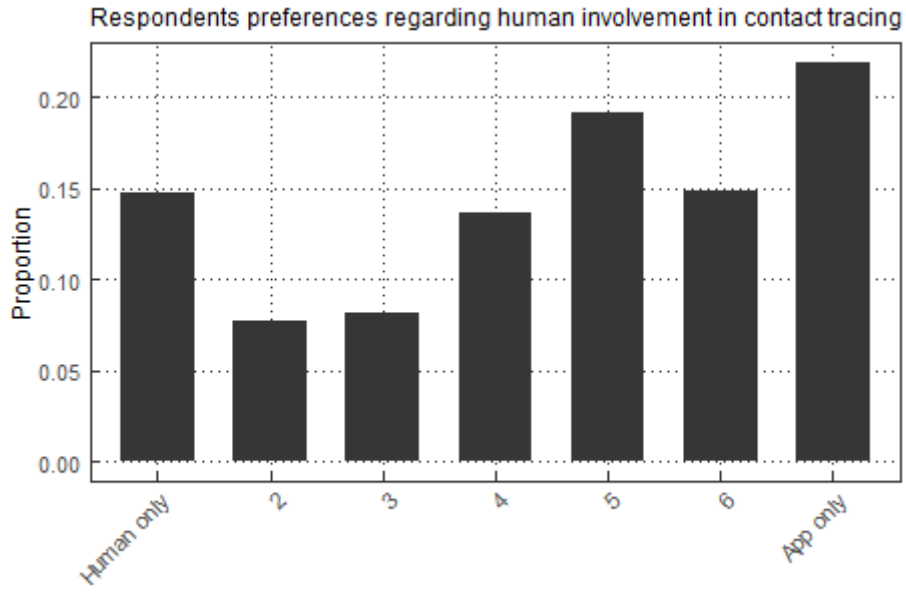


Fig. C5: Overview of preferences about human vs. digital contact tracing

Appendix D: References

Berinsky, A. J., Margolis, M. F., & Sances, M. W. (2014). Separating the shirkers from the workers? Making sure respondents pay attention on self-administered surveys. *American Journal of Political Science*, 58(3), 739-753.

Troncoso, C., Payer, M., Hubaux, J. P., Salathé, M., Larus, J., Bugnion, E., ... & Barman, L. (2020). Decentralized privacy-preserving proximity tracing. arXiv preprint: arXiv:2005.12273.

Veale, M. (2020). Analysis of the NHSX Contact Tracing App 'Isle of Wight' Data Protection Impact Assessment. OSF Preprint: https://osf.io/preprints/lawarxiv/6fvgh

Downloaded from https://www.cambridge.org/core. University of Exeter, on 25 Sep 2020 at 08:35:03, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/XPS.2020.30