Public acceptance of Privacy-Encroaching Policies to Address the COVID-19 Pandemic in the United Kingdom

Stephan Lewandowsky[1,2], Simon Dennis[3], Amy Perfors[3], Yoshihisa Kashima[3], Josh White[3], Paul Garrett[3], Daniel R. Little[3], & Muhsin Yesilada[1]

[1] University of Bristol

[2] University of Western Australia

[3] University of Melbourne

Author Note

This work was supported by the Elizabeth Blackwell Institute, University of Bristol, with funding from the University's alumni and friends.

Correspondence concerning this article should be addressed to Stephan Lewandowsky, School of Psychological Science, Cabot Institute, 12A Priory Road, University of Bristol, Bristol BS8 1TU, United Kingdom. E-mail: stephan.lewandowsky@bristol.ac.uk; web: http://www.cogsciwa.com.

Abstract

The nature of the COVID-19 pandemic may require governments to use privacy-encroaching technologies to help contain its spread. One technology involves co-location tracking through mobile Wi-Fi, GPS, and Bluetooth to permit health agencies to monitor people's contact with each other, thereby triggering targeted social-distancing when a person turns out to be infected. The effectiveness of tracking relies on the willingness of the population to support such privacy encroaching measures. We report the results of two large surveys in the United Kingdom, conducted during the peak of the pandemic, that probe people's attitudes towards various tracking technologies. The results show that by and large there is widespread acceptance for co-location tracking. Acceptance increases when the measures are explicitly time-limited and come with opt-out clauses or other assurances of privacy. Another possible future technology to control the pandemic involves "immunity passports", which could be issued to people who carry antibodies for the COVID-19 virus, potentially implying that they are immune and therefore unable to spread the virus to other people. Immunity passports have been considered as a potential future step to manage the pandemic. We probe people's attitudes towards immunity passport and find strong opposition as well as strong support.

Keywords: keywords

Word count: X

Public acceptance of Privacy-Encroaching Policies to Address the COVID-19 Pandemic in the United Kingdom

The COVID-19 pandemic has changed nearly all aspects of people's lives ~~around the world~~. In the absence of a vaccine or successful treatments, the only tools available to control the pandemic are behavioral in nature (Habersaat et al., 2020). Countries that have successfully "flattened the curve" have primarily resorted to social-distancing measures. However, social distancing cannot be sustained indefinitely, which raises the question about how social life can resume without reigniting the pandemic. This question has become particularly acute at the time of this writing (July 2020), as countries around the world are struggling to prevent a "second wave" of the pandemic. At least two potential technological or biomedical options have been developed to assist with management of the relaxation of social distancing. The first option involves the use of tracking technologies, which monitor people's interactions and send alerts to people who have been in proximity to others who turn out to be infected (see, e.g., Oliver et al., 2020). This technology has matured to the point where several countries, among them Singapore, Germany, and Australia, have rolled out tracking technologies at scale. The second option remain impractical at present and involves issuing people with "immunity passports" if they test positive for antibodies, indicating their presumed immunity to the virus.

Tracking technologies

Several tracking "apps" exist for use in smartphones, although they differ in where and how they store the contact information. Some tracking apps are based on transmitting geolocation to a central server, and if a person turns out to be infected, all other persons they encountered during the previous critical time period are identified and alerted via text message. Other apps rely on Bluetooth to make a note of other mobile phones nearby, and contacts of people who turn out to be infected are notified without their geo-location or identity being recorded on a central server.

At the policy level in the United Kingdom, multiple developments and analyses have cleared the way for the impending introduction of a tracking app. Although the Coronavirus Bill (https://services.parliament.uk/Bills/2019-21/coronavirus/documents.html) passed on 25 March 2020 did not include any provisions for wider surveillance tracing, public health enforcement in the U.K. has existing widespread power to request contact data for infectious or potentially infectious persons. The Information Commissioners' Office (ICO) has opined that use of mobile phone data would be legal (https://www.theguardian.com/world/2020/mar/27/watchdog-approves-use-uk-phone-data-if-helps-fight-coronavirus) if broader contact-tracing were introduced (presumably by legislation). The ICO also acknowledged that anonymous geolocation data is already being used to fight the pandemic and approved its use (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/statement-in-response-to-the-use-of-mobile-phone-tracking-data-to-help-during-the-coronavirus-crisis/).

However, all existing tracking technologies come with wide-ranging implications for people's privacy. The implications of "public-health surveillance" have stimulated much concern among some scholars (e.g., French & Monahan, 2020), and in the U.K., more than 170 cybersecurity and privacy experts have signed an open letter (https://www.businessinsider.com/cybersecurity-experts-uk-government-contact-tracing-surveillance-2020-4?r=US&IR=T) warning the government against use of any tracking app for mass surveillance.[1]

Those concerns may also be shared by the public, which in most countries is known to place sonsiderable value on their privacy. In a survey of the public in 27 contries within the European Union, Skinner, Cameron, and Friedewald (2014) found that 87% of the public found protection of their privacy to be important or very important. Similarly, in a more recent survey in Germany, 82% of respondents claimed that they are very or at least

[1] The first author of this article was a signatory of that letter.

somewhat concerned about their data privacy (Kozyreva, Herzog, Lorenz-Spreen, Hertwig, & Lewandowsky, 2020). One might therefore expect the public to be concerned about the invasion of privacy that is a nearly inevitable by-product of any COVID-related tracking technology.

There are, however, at least two exceptions to the public's concern about privacy. First, people in the European Union generally endorse the reuse of health data for the common good, although they are concerned about commercialization (Skovgaard, Wadmann, & Hoeyer, 2019). Second, it is well known that people's actual privacy-related behaviors seem to stand in contrast to their attitudes. This gap has become known as the "privacy paradox" (e.g., Acquisti, Brandimarte, & Loewenstein, 2015; Barth & de Jong, 2017; Kokolakis17; Norberg, Horne, & Horne, 2007). For example, in the survey by Kozyreva et al. (2020), few respondents indicated that they take steps to protect their privacy online: Just 37% adjust privacy and ad settings on online platforms, and 20% do not use any privacy-enhancing tools.

The privacy paradox has been attributed to a variety of factors, including the fact that people's concerns about privacy are highly context dependent (Acquisti et al., 2015). For example, it has been proposed that people engage in a "privacy calculus", such that people will self-disclose personal information, for example by using social media, so long as the perceived benefits exceed the perceived negative consequences (Dienlin & Metzger, 2016). In light of the current health risks emerging from the COVID pandemic, people's context-sensitive privacy calculus may therefore override their over-arching concerns about privacy.

Immunity passports

Although at present immunity passports do not exist, they are within reach as serological tests are becoming available, although to date their reliability has been insufficient (Voo, Clapham, & Tam, 2020). The ethical implications of immunity passports are hotly debated in the literature (Hall & Studdert, 2020; Kofler & Baylis, 2020; Persad & Emanuel, 2020, ' @Studdert20). The primary concern involves the implications of immunity, which free the person from being subjected to social distancing measures because they are presumed not to be infectious themselves. Conversely, people who are not immune may be confined to their homes and locked out of society (Kofler & Baylis, 2020).

Historical precedent from the 19th century suggests that this division of society into those who are immune and those who are not can have dystopian consequences—affecting all aspects of life, from choice of job to choice of romantic partners (Kofler & Baylis, 2020). In addition to stratifying along a new dimension of biologically-determined "haves" and "have nots", the mere existence of immunity passports would also trigger an erosion of privacy because passports can only be useful to the extent that their holders are monitored and checked. Passports may also ironically create a risk to public health: If the privileges associated with immunity are sufficiently great, there may be sufficient incentive for people to seek self-infection with the virus (Kofler & Baylis, 2020). Some scholars have therefore argued that "this idea has so many flaws that it is hard to know where to begin" (Kofler & Baylis, 2020).

On the other side of the ledger, some scholars have argued that under certain circumstances, immunity passports may be ethical, provided sufficient safeguards are put in place (Hall & Studdert, 2020; Persad & Emanuel, 2020; Studdert & Hall, 2020; Voo et al., 2020). For example, it has been argued that certification of one's immunity status may spur people into greater prosocial altruism, for example by taking on riskier treatment roles or donating blood (Hall & Studdert, 2020). Another suggestion has been to prioritize critical or high-risk sectors of society (e.g., health care workers) for testing and to issue immunity passports only to people within that sector, thus limiting inequities to people whose welfare is deemed to be of particular interest to society overall (Voo et al., 2020).

In light of this ethical controversy, an understanding of the public's views and concerns is particularly urgent. This article reports the results from two large-scale surveys conducted in the United Kingdom during the height of the pandemic (March-April 2020) that probed the public's attitude towards both privacy-encroaching options to combat the pandemic: tracking technologies and immunity passports. The surveys presented people with one of several different possible tracking policies, each accompanied by different policy options (e.g., a sunset clause). We also collected a variety of attitude measures, such as people's worldviews, trust in government, and their risk perception relating to COVID, to identify potential predictors of policy acceptance.

Method

Overview

The two survey waves were conducted roughly three weeks apart and were materially identical, with differences noted below. The preregistration for the first survey wave can be found at https://osf.io/d3pcn. The second wave inherited the same preregistration. The surveys reported here are part of a larger, international project that involved data collection in 7 countries (U.K., Australia, U.S.A., Germany, Taiwan, and Switzerland). A continually-updated summary of the overall project is available at https://stephanlewandowsky.github.io/UKsocialLicence/index.html.

The first wave included two tracking scenarios: one in which the public had to opt in voluntarily (called the "mild" scenario from here on), and one in which all mobile users were mandated to participate and the government could issue quarantine orders for individuals ("severe"). The second wave additionally included a third scenario ("Bluetooth"), in which people's phones exchanged messages anonymously whenever they were in proximity, thus permitting alerting people who may have been infected without the government knowing who they are or where they were. Use of this app was voluntary.

Participants

The first survey was conducted on 28 and 29 March 2020 and involved a representative sample of 2,000 U.K. participants, recruited through the online platform Prolific (https://www.prolific.co/). Participants were at least 18 years old and were paid 85 Pence for their participation in the 10-minute study. At the time, there were 14,543 confirmed cases of COVID-19 in the U.K., with 1,161 deaths (https://ourworldindata.org/coronavirus).

The second wave was conducted on 16 April and involved another Prolific representative sample of 1,500 participants. Participants were paid GBP 1.34 for their participation in the (approximately) 15-minute study. This was equivalent to GBP 5.98 per hour based on the average observed completion time. At the time of the second wave, there were 98,476 confirmed cases of COVID-19 in the U.K., with 14,915 deaths attributed to the disease (https://ourworldindata.org/coronavirus).

Instrument and procedure

Verbatim copies of the surveys are available at https://osf.io/d3pcn (for the first wave) and https://osf.io/pw5yj/ (for the second wave). Figure 1 provides an overview of the survey instrument used in both waves. Each white box represents a block with one or more questions pertaining to that topic or construct. Numbers next to the white boxes indicate the number of items in that block. The black boxes represent the different tracking scenarios being tested. Comprehension questions immediately after the scenario and a free text box at the very end of survey (for additional comments) are not shown.

Participants first responded to items that probed their perceived risk from COVID-19 itself. Those items are shown in Table 1. The table displays the core question for each item: the exact wordings differed slightly between waves and scenarios and are available in the full survey texts. All responses used a 5-point scale, where higher values always corresponded to endorsement of the issue being probed (e.g., 1 = Not at all concerned to 5 = Extremely concerned). The labels and endpoints differed slightly between items and are available in the full survey texts. Participants were then randomly assigned to scenarios in each wave and were presented with the scenario text.

The text of the mild scenario was:

> The COVID-19 pandemic has rapidly become a worldwide threat. Containing the virus' spread is essential to minimise the impact on the healthcare system, the economy, and save many lives. The U.K. Government might consider using smartphone tracking data to identify and contact those who may have been exposed to people with COVID-19. This would help reduce community spread by identifying those most at risk and allowing health services to be appropriately targeted. Only people who downloaded a government app and agreed to be tracked and contacted would be included in the project. The more people download and use this app, the more effectively the Government would be able to contain the spread of COVID-19. Data would be stored in an encrypted format on a secure server accessible only to the U.K. Government. Data would only be used to contact those who might have been exposed to COVID-19.

The severe scenario was:

> The COVID-19 pandemic has rapidly become a worldwide threat. Containing the virus' spread is essential to minimise the impact on the healthcare system, the economy, and save many lives. The U.K. Government might consider using phone tracking data supplied by telecommunication companies to identify and contact those who may have been exposed to people with COVID-19. This would help reduce community spread by identifying those most at risk and allowing health services to be appropriately targeted. All people using a mobile phone would be included in the project, with no possibility to opt-out. Data would be

stored in an encrypted format on a secure server accessible only to the U.K. Government which may use the data to locate people who were violating lockdown orders and enforce them with fines and arrests where necessary. Data would also be used to inform the appropriate public health response and to contact those who might have been exposed to COVID-19. Individual quarantine orders could be made on the basis of this data.

The Bluetooth scenario, used in the second wave only, was:

The COVID-19 pandemic has rapidly become a worldwide threat. Containing the virus' spread is essential to minimise the impact on the healthcare system, the economy, and save many lives. Apple and Google have proposed adding a contact tracing capability to existing smartphones to help inform people if they have been exposed to others with COVID-19. This would help reduce community spread of COVID-19 by allowing people to voluntarily self-isolate. When two people are near each other, their phones would connect via bluetooth. If a person is later identified as being infected, the people they have been in close proximity to are then notified without the government knowing who they are. The use of this contact tracing capability would be completely voluntary. People who are notified would not be informed who had tested positive.

People's acceptability of the scenario was then probed 4 times (see left-most column in Figure 1). The initial test was immediately after presentation of the scenario. The wording of the acceptability question differed between scenarios to reflect the attributes of the policy. For the mild scenario, the question asked whether a participant "would download and use" the app, whereas for the severe scenario the question was whether the "use of tracking data in this scenario acceptable." For the Bluetooth scenario, the participant was asked whether they "would use" the capability.

The second test occurred after a number of intervening questions that probed the perceived benefits of the tracking app described in the scenario, as well as the risks and harms that could arise from release of the personal data gathered in the process. Those items are shown in Table 2. The table again displays the core question for each item, with the exact wording available in the survey texts. All responses used a 6-point scale, where higher values always corresponded to endorsement of the issue being probed by the item (e.g., 1 = Not at all to 6 = Extremely). Items of differing polarity are identified by "[R]" in the table and were reverse scored before computing aggregate scores. For example, the items probing difficulty of declining participation and having control of their data are of different polarity because a consistent position would imply endorsement of one and rejection of the other. The scale labels and endpoints differed slightly between items and are available in the full survey texts.

The second test of acceptability was immediately followed by two more items that again queried acceptance of the scenario~~,~~ but under modified assumptions. Those items were only presented to participants who found the scenario unacceptable on the second occasion. The first modification involved a sunset clause and queried whether deletion of the data after 6 months would make the scenario acceptable. The second modification differed betweeen scenarios and queried acceptability if the data were stored locally rather than on a government server (mild) or if users could opt out of data collection (severe). This second modified assumption was not ~~queried~~ in the Bluetooth scenario because it already involved local storage and voluntary participation.

Assessement of acceptability was followed by an assessment of people's political worldviews, using three items that probed endorsement of free markets and small government (greater agreement reflects more conservative-libertarian worldviews).

In the second wave, the worldview questions were preceded by a series of questions that probed people's attitudes to "immunity passports." Immunity passports were explained as follows:

> An “immunity passport” indicates that you have had a disease and that you have the antibodies for the virus causing that disease. Having the antibodies implies that you are now immune and therefore unable to spread the virus to other people. Thus, if an antibody test indicates that you have had the disease, you could be allocated an immunity passport which would subsequently allow you to move around freely. Immunity passports have been proposed as a potential step towards lifting movement restrictions during the COVID-19 pandemic.

Table 3 explains the items used to query attitudes towards immunity passports. The table again displays the core question for each item, with the exact wording available in the survey text for wave 2. Responses used a 5-point or 6-point scale, where higher values always corresponded to endorsement of the issue being probed (e.g., 1 = Not at all to 6 = Extremely). The final column in the table indicates the scale (5 or 6 points) for each item. Items of different polarity that required reverse scoring before being aggregated into a composite score are identified by “[R]”.

Altogether the surveys contained 32 (first wave) and 43 items (second wave), including one attention filter presented immediately after the scenario that tested participants' comprehension of the gist of each scenario. Because some questions were contingent on earlier responses, not all participants saw all items. Not all items in the surveys are analyzed and reported here.

Participants were invited to enter the survey through a link placed on Prolific. After providing informed consent, participants responded to the items in the sequence shown in Figure 1. The survey concluded with debriefing information that included links to official websites with information about COVID-19 and resources for assistance for anxiety or other mental health concerns relating to the pandemic.

Results

Data and source code availability

The data are available at https://osf.io/42wj6/ (first wave) and (https://osf.io/pw5yj/(second wave). Demographics and other sensitive variables (such as location information) that could lead to deanonymization have been omitted from the published data sets. The source code for analysis is embedded in the report at https://stephanlewandowsky.github.io/UKsocialLicence/index.html.

Data preparation and demographics of sample

The requested number of participants was not obtainable in either wave in a reasonable time. The survey was discontinued after approximately 24 hours had elapsed since the last response was collected, which yielded a sample of N=1987 and N=1493 for the first and second wave, respectively. After removal of duplicate responses from the same Prolific ID (N=142 and 1 and N=1 and 1, respectively, for wave 1 and 2), participants who failed the comprehension check, and incomplete responses, the final sample retained for analysis contained N=1810 and N=1446 for wave 1 and 2, respectively. The large number of duplicate responses in wave 1 arose from the need to run the survey in two batches on consecutive days because Prolific does not permit samples greater than 1,500. The second wave was run in a single batch but included a question whether a participant had taken the survey before. 174 respondents indicated yes, and a further 131 were unsure. Given the 3-week lag between waves, all those responses were retained for the second wave. Basic demographics are shown in Table 4 for both waves.

Self-reported education level is shown in Table 5. Samples from both waves were remarkably similar, although in both instances people with university education were over-represented.

Perceived risk from COVID-19

Figure 2 shows the distribution of responses to the 4 items querying people's perceived risk from COVID-19 for both waves. The items are explained in Table 1. The figure shows that there were only small differences between the two waves. On both occasions, people expressed considerably more concern for others than for themselves.

Attitudes towards tracking scenarios

The first part of the analysis focused on the various tracking policies sketched in the scenario presented to participants.

Overall acceptability of scenarios. Figure 3 shows acceptability ratings for the first wave of the survey, and Figure 4 shows the same ratings for the second wave. The four groups of bars in each figure refer to the 4 occasions on which acceptability was queried in the survey (see Figure 1). The last two items were only presented to participants who found the scenario unacceptable at the second test. The bars in the figure for those items represent the acceptable responses from the second test and the *additional* acceptance elicited by addition of a sunset clause and/or local storage or opt-out.

Overall, acceptance of tracking technologies was quite high, with a baseline at the initial test of around 70% for the mild and Bluetooth scenarios, and above 60% for the severe scenario. Acceptance of all scenarios declines slightly at the second test, after participants have responded to more detailed questions about benefits and potential harms of the scenarios (reported next). The addition of a sunset clause boosts acceptance for all scenarios, as does the provision of local storage (for mild) and opt-out (severe). Indeed, with an opt-out clause, the severe scenario reaches nearly 90% acceptance. It must be borne in mind, however, that the severe scenario with an opt-out clause no longer meaningfully differs from the mild scenario.

Potential effectiveness of tracking. Figure 5 shows responses from both waves to three questions about the perceived benefits of the tracking scenario. The panels and Y-axes use the labels from Table 2. It is clear that the severe scenario is judged to be slightly, but not dramatically, more effective than the other two for at least some of the items. The two waves do not appear to differ appreciably from each other.

Separate one-way ANOVAs for each wave and item confirm the pattern in the figure, with an effect of scenario type on Reduce Contracting in wave 1, $F(1, 1,808) = 5.60$, $MSE = 1.88$, $p = .018$, $\hat{\eta}^2_G = .003$, and in wave 2, $F(2, 1,443) = 13.13$, $MSE = 1.75$, $p < .001$, $\hat{\eta}^2_G = .018$. Follow-up comparisons by Tukey HSD revealed that the severe scenario differed from each of the others in wave 2, whereas the mild and Bluetooth scenarios did not differ from each other. For Resume Normal, scenario type had no effect in wave 1, $F(1, 1,808) = 0.84$, $MSE = 1.93$, $p = .360$, $\hat{\eta}^2_G = .000$, but it did have an effect in wave 2, $F(2, 1,443) = 5.01$, $MSE = 1.81$, $p = .007$, $\hat{\eta}^2_G = .007$, which arose from a significant difference between the severe and Bluetooth scenarios. No other pairwise tests were significant. Finally, for Reduce Spread, scenarios differed significantly in wave 1, $F(1, 1,808) = 5.63$, $MSE = 1.91$, $p = .018$, $\hat{\eta}^2_G = .003$, and wave 2, $F(2, 1,443) = 8.06$, $MSE = 1.70$, $p < .001$, $\hat{\eta}^2_G = .011$, with the difference in wave 2 arising from the severe scenario leading to significantly higher confidence than the other two scenarios, which did not differ from each other.

Potential harms from tracking. The items probing harm (Table 2) were aggregated into three clusters that represented, respectively, people's perceived control over the policy (Items Difficult decline [R] and Have control), harms from the policy (Sensitivity, Risk of tracking, Data security [R]), and trust in government (Proportionality, Trust intentions, Trust privacy). Items within each cluster were averaged after reverse scoring where appropriate (items identified with [R]).

Figure 6 shows responses from both waves to the three clusters of questions about the perceived harms of the different tracking technologies. Each panel presents the composite score for each cluster of items.

Separate one-way ANOVAs were conducted for each wave and item cluster where appropriate. For the control cluster, the severe scenario was omitted from any analysis because—quite appropriately—most people recognized that it offered no control at all. The only ANOVA for the control cluster thus involved a comparison between the mild scenario and Bluetooth in wave 2, $F(1, 958) = 1.80$, $MSE = 0.76$, $p = .180$, $\hat{\eta}^2_G = .002$, which revealed that the two scenarios did not difer from each other. For harms, differences between scenarios were significant for wave 1, $F(1, 1, 808) = 37.49$, $MSE = 1.12$, $p < .001$, $\hat{\eta}^2_G = .020$, as well as for wave 2, $F(1, 1, 808) = 37.49$, $MSE = 1.12$, $p < .001$, $\hat{\eta}^2_G = .020$, with the latter effect being exclusively driven by a difference between the severe and mild scenarios. For trust, effectis were observed in wave 1, $F(1, 1, 808) = 20.96$, $MSE = 1.90$, $p < .001$, $\hat{\eta}^2_G = .011$, and wave 2, $F(2, 1, 443) = 9.62$, $MSE = 1.68$, $p < .001$, $\hat{\eta}^2_G = .013$, with the latter effect being driven by significant differences between the mild scenario and each of the other two.

Predictors of tracking policy acceptance. The final analysis modeled acceptance of the various policy scenarios as a function of several sets of predictors using logistic regression. The predictors included wave (first or second), demographics (age and gender, excluding respondents who did not choose "male" or "female"; $N = 6$), a measure of worldview aggregated across the three relevant items; perceived risk from COVID (aggregated score across items in Table 1); and the earlier aggregate scores for perceived harm from the policy and trust in government (top two panels of Figure 6; the bottom panel relating to control was omitted because there was no meaningful variance for the severe scenario). In addition, the type of scenario was included in the model as an experimental variable. The initial acceptance of the scenario (i.e., the first time acceptance was probed) was used as the binary dependent variable.

We first attempted to fit a number of random effects models (e.g., with a different intercept for each participant) using the *lmer* function in R. All of these models failed to converge. The likely reason for this failure was near-zero variance of the random effect. We therefore fit a conventional logistic regression using *glm* in R with fixed effects only.

We compared two fixed-effect models: a complex model which included the above predictors and their interactions with wave, and a simpler model without any interaction terms. Removing the interactions incurred no significant loss of fit, $\chi^2(7) = 1.90$, $p > .10$. Moreover, the simpler model was preferred by BIC (2806 vs. 2861). We therefore only report the simpler model with wave functioning as a predictor but not interacting with any of the others. Figure 7 shows the estimated standardized regression coefficients for the final model (intercept omitted from figure). The model accounted for a substantial share of the variance, McFadden's pseudo-r^2=0.33 and Cragg and Uhler's pseudo-r^2=0.48.

The figure shows that increasing age was associated with reduced acceptance of a policy, and that men were less accepting than women overall. In addition, worldview had a small but consistent effect on policy acceptance, such that people with a more conservative or libertarian orientation were slightly less likely to accept any of the policies. Reduced acceptance was also associated with greater perceived harms from the tracking technologies. Conversely, greater perceived risk from COVID was associated with greater policy acceptance. Finally, by far the most important predictor turned out to be trust in government. People who trust the government to safeguard privacy were considerably more likely to accept the policies than people who distrust the government.

Immunity passports

The second part of the analysis focused on attitudes towards immunity passports. This analysis is confined to wave 2 because questions about passports were limited to that wave.

Acceptance of immunity passports. Figure 8 displays the distribution of responses to all items querying immunity passports. The majority of people clearly did not object to the idea of passports, with concern being low on average and more than 60% of people wanting one for themselves to varying extents. There were, however, around 20% of respondents who considered passports to be unfair and who opposed them completely (response category 1 for the second support item).

Predictors of immunity passport acceptance. To model acceptance of immunity passports we created a composite score for immunity passports by averaging across all items in Table 3, reverse scoring where necessary. The "Infect self" item was excluded because it exhibited little variance and also did not correlate appreciably with most of the other items. The composite score was used as the dependent variable in a linear regression model that included most of the predictors from before; namely, age, gender (again excluding responses other than "male" or "female"), worldviews, perceived risk from COVID-19, and the perceived harms of the tracking policy and trust in government relating to that policy. Note that the latter two measures were gathered in connection with the tracking policy rather than immunity passports.

Figure 9 shows the regression coefficients for this model. The model accounted for a moderate share of variance, r^2=0.17, adjusted r^2=0.17. Most of the variance accounted for was due to the two predictors relating to the tracking scenario (Perceived harms and Trust in government). When they were removed from the model, the explained variance was small, r^2=0.03, adjusted r^2=0.02, although age retained its significant effect, $t(1439) = 4.16$, $p < .001$, and the effect of perceived risk from COVID-19 was now highly significant, $t(1439) = 3.31$, $p = .001$.

In contrast to the tracking policies, increasing age was associated with increased acceptance of immunity passports whereas gender had no effect here. The other predictors relating to perceived risks predicted attitudes towards immunity passports as one might expect: greater perceived risk of the disease and greater trust in government were associated with more favorable attitudes whereas skepticism towards the tracking policies was also associated with greater skepticism towards immunity passports.

Discussion

Limitations and relationship to previous results

Our surveys only included three different tracking scenarios, which is a small number relative to the total number of technological solutions now available (https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/). We also presented scenarios that differed somewhat from those currently in use around the world.

Nonetheless our tracking results mesh extremely well with those reported by an independent team of authors in the U.K. (Abeler, Altmann, Milsom, Toussaert, & Zillessen, 2020). Similar to both our survey waves, Abeler et al. (2020) found that up to 75% of respondents would install the app. One difference between the studies is that we specified data storage and access precisely, whereas Abeler et al. (2020) did not explicity explain where the data would be held (i.e., locally without location information or centrally). Their scenario was, however, closest to our Bluetooth scenario, which renders the two sets of acceptance probabilities nearly identical.

We are not aware of any other data on people's acceptance of immunity passports.

Implications for policy

Our results have clear implications for policy. Perhaps the most important finding is the high overall level of endorsement for both policy options: A majority of people supports immunity passports, and an even greater majority endorses tracking-based policies. This high level of endorsement stands in contrast to people's commonly professed concern for their privacy (Barth & de Jong, 2017). It appears that the British public is prepared to sacrifice some privacy in the interest of public health.

A second implication of our results is that the details of the policy arguably mattered little: In both waves, the initial acceptance of the mild scenarion was only 5% – 10% greater than acceptance of the draconian severe scenario. That said, acceptance increased considerably with the simple addition of a sunset clause.

A further important aspect of our result is that the issue did not appear to be highly politicized. Although people with a conservative-libertarian worldview were less likely to accept tracking technologies (while being slightly more likely to endorse immunity passports), the effect sizes were modest relative to indicators of perceived risk from COVID, harm from the tracking policy, and most important, trust in the government to safeguard people's data.

These implications can be combined into a straightforward policy for tracking apps: People are relatively unconcerned about where the data are stored, but they do care about how long the data will be stored for. Any policy should be accompanied by a clear sunset clause. In addition, given the important role of trust, any policy rollout should be accompanied by clear messages about why and how the government is a trustworthy custodian of people's data.

References

Abeler, J., Altmann, S., Milsom, L., Toussaert, S., & Zillessen, H. (2020). *Support in the UK for app-based contact tracing of COVID-19*. Oxford: Unpublished manuscript.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*, 509–514. doi:10.1126/science.aaa1465

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox — investigating discrepancies between expressed privacy concerns and actual online behavior — a systematic literature review. *Telematics and Informatics*, *34*, 1038–1058. doi:10.1016/j.tele.2017.04.013

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. sample. *Journal of Computer-Mediated Communication*, *21*, 368–383. doi:10.1111/jcc4.12163

French, M., & Monahan, T. (2020). Dis-ease surveillance: How might surveillance studies address COVID-19? *Surveillance & Society*, *18*(1). doi:10.24908/ss.v18i1.13985

Habersaat, K. B., Betsch, C., Danchin, M., Sunstein, C. R., Böhm, R., Falk, A., … Butler, R. (2020). Ten considerations for effectively managing the COVID-19 transition. *Nature Human Behaviour*. doi:10.1038/s41562-020-0906-x

Hall, M. A., & Studdert, D. M. (2020). Privileges and immunity certification during the COVID-19 pandemic. *JAMA*. doi:10.1001/jama.2020.7712

Kofler, N., & Baylis, F. (2020). Ten reasons why immunity passports are a bad idea. *Nature*, *581*, 379–381. doi:10.1038/d41586-020-01451-0

Kozyreva, A., Herzog, S., Lorenz-Spreen, P., Hertwig, R., & Lewandowsky, S. (2020). Artificial intelligence in online environments: Representative survey of public attitudes in germany. doi:10.17617/2.3188061

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*, 100–126. doi:10.1111/j.1745-6606.2006.00070.x

Oliver, N., Lepri, B., Sterly, H., Lambiotte, R., Delataille, S., Nadai, M. D., … Vinck, P. (2020). Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. *Science Advances*, eabc0764. doi:10.1126/sciadv.abc0764

Persad, G., & Emanuel, E. J. (2020). The ethics of COVID-19 immunity-based licenses (“immunity passports”). *JAMA*, *323*, 2241–2242. doi:10.1001/jama.2020.8102

Skinner, G., Cameron, D., & Friedewald, M. (2014). *The PRISMS survey*. Fraunhofer Institut. Retrieved from http://publica.fraunhofer.de/documents/N-410740.html

Skovgaard, L. L., Wadmann, S., & Hoeyer, K. (2019). A review of attitudes towards the reuse of health data among people in the European Union: The primacy of purpose and the common good. *Health Policy*, *123*, 564–571. doi:10.1016/j.healthpol.2019.03.012

Studdert, D. M., & Hall, M. A. (2020). Disease control, civil liberties, and mass testing calibrating restrictions during the Covid-19 pandemic. *New England Journal of Medicine*. doi:10.1056/nejmp2007637

Voo, T. C., Clapham, H., & Tam, C. C. (2020). Ethical implementation of immunity passports during the COVID-19 pandemic. *The Journal of Infectious Diseases*. doi:10.1093/infdis/jiaa352

Table 1

Items querying risks from COVID-19

Question	Label
How severe do you think novel coronavirus (COVID-19) will be for the general population?	General harm
How harmful would it be for your health if you were to become infected COVID-19?	Personal harm
How concerned are you that you might become infected with COVID-19?	Concern self
How concerned are you that somebody you know might become infected with COVID-19?	Concern others

Table 2

Items querying potential benefits (Bfit) and harms (Harm) of app

Item	Question	Label
Bfit 1	How confident are you that the Government app would reduce your likelihood of contracting COVID-19?	Reduce contracting
Bfit 2	How confident are you that the Government app would help you resume your normal activities more rapidly?	Resume normal
Bfit 3	How confident are you that the Government app would reduce the spread of COVID-19?	Reduce spread
Harm 1	How difficult is it for people to decline participation?	Difficult decline [R]
Harm 2	To what extent do people have ongoing control of their data?	Have control
Harm 3	How sensitive is the data being collected?	Sensitivity
Harm 4	How serious is the risk of harm from the proposed policy?	Risk of tracking
Harm 5	How secure is the data that would be collected?	Data security [R]
Harm 6	To what extent is the Government only collecting the data necessary to achieve the purposes of the policy?	Proportionality
Harm 7	How much do you trust the Government to use the tracking data only to deal with the COVID-19 pandemic?	Trust intentions
Harm 8	How much do you trust the Government to be able to ensure the privacy of each individual?	Trust privacy

Table 3

Items querying attitudes towards immunity passports

Question	Label	Scale
Would you support a government proposal to introduce immunity passports?	Support	6
How concerned are you about the idea of introducing an immunity passport?	Concern [R]	5
How much would you like to be allocated an immunity passport?	Like self	6
To what extent do you believe an immunity passport could harm the social fabric?	Harm general [R]	6
Is it fair for people with immunity passports to go back to work, while individuals without a passport cannot?	Fairness	6
To what extent would you consider infecting yourself with COVID-19 to get an immunity passport?	Infect self	6
Would you support a government proposal to introduce immunity passports?	Support 2	6

Table 4

Demographics for both waves .

	Gender			Age	
Wave	Male	Female	Other	Mean	SD
Wave 1	48.80%	51%	0.10%	45.60	15.36
Wave 2	48.20%	51.70%	0.10%	46.15	15.32

Table 5

Self-reported level of education for both waves .

	Education			
Wave	GCSE	A levels/VCE	University	Apprent/Vocatnl
Wave 1	15.30	17.30	55.60	11.70
Wave 2	14.60	17.20	56.40	11.80

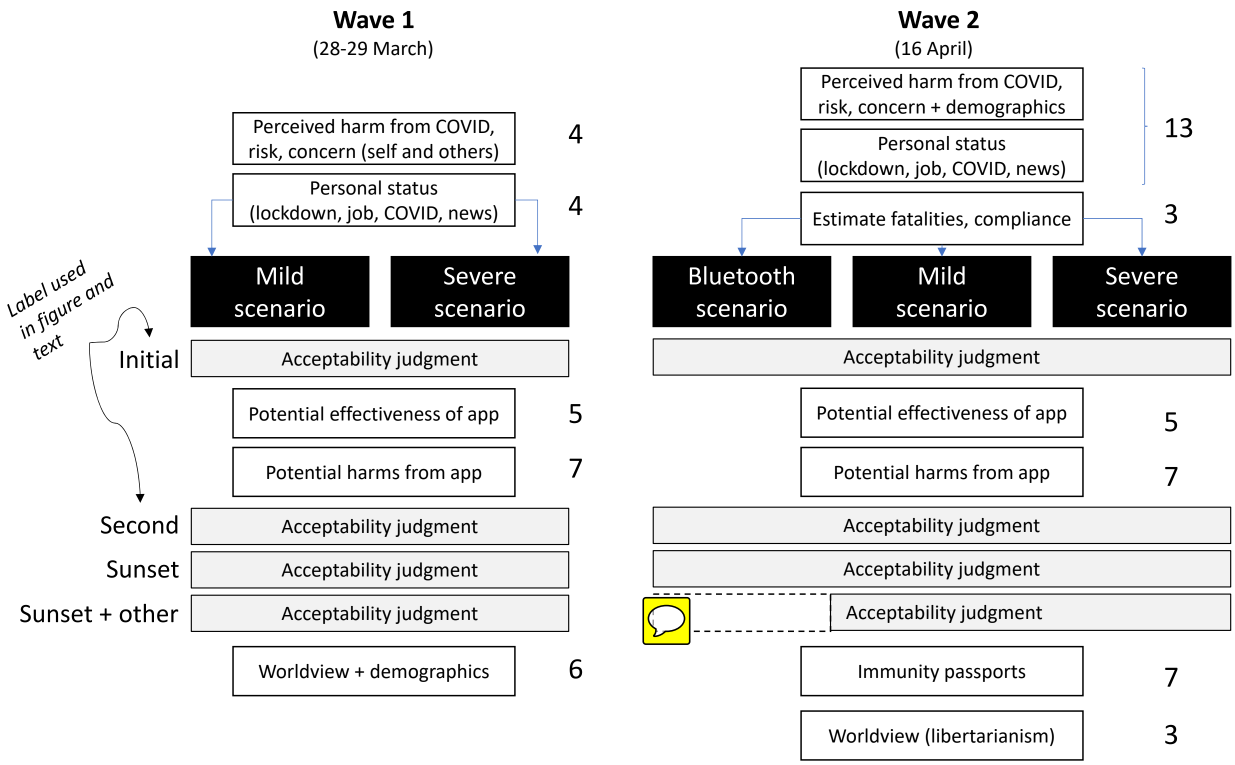

Figure 1. Overview of surveys used in both waves.

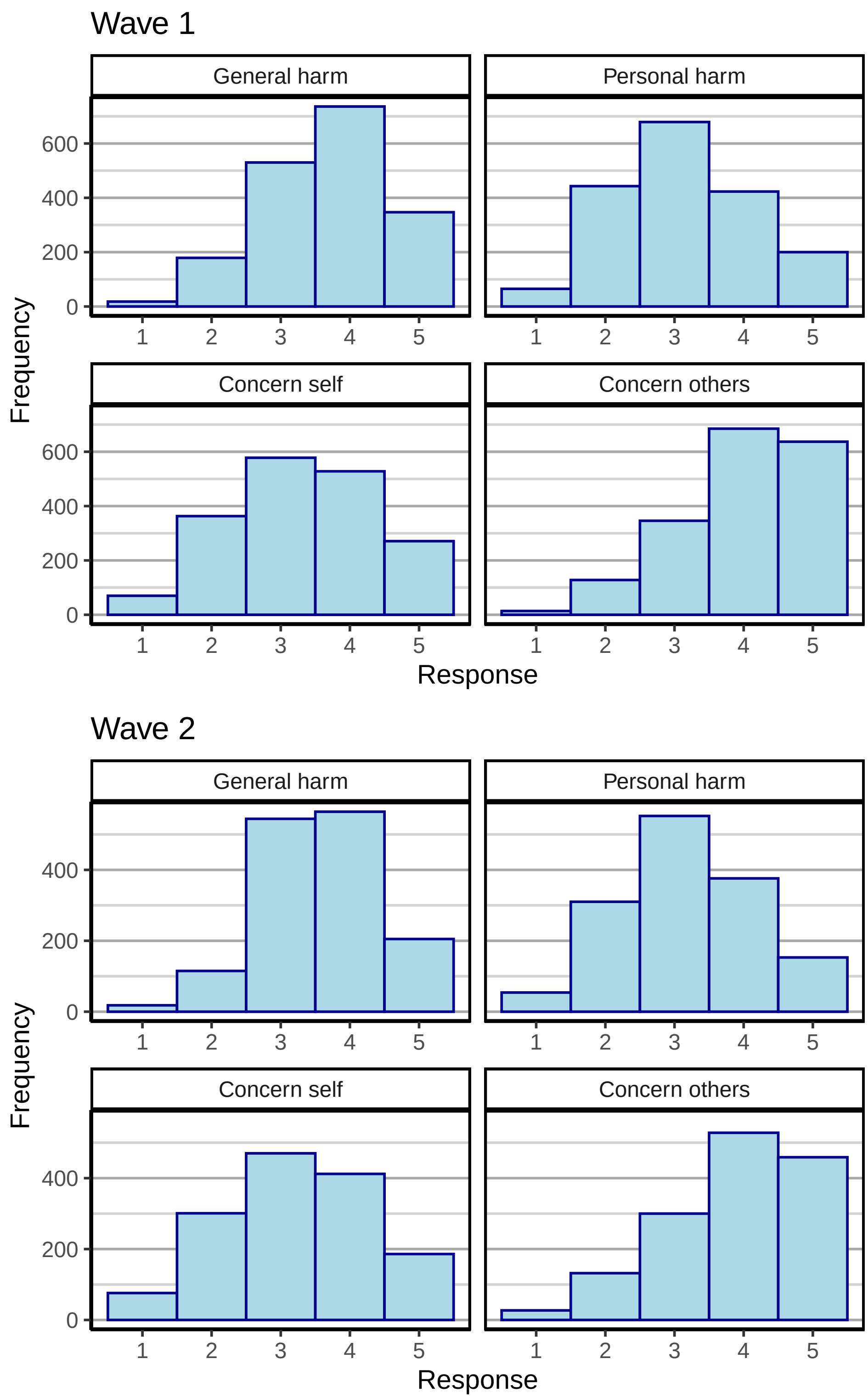

Figure 2. Perceived risk from COVID during the first wave (28-29 March 2020; top set of panels) and during the second wave (16 April 2020; bottom panels). Each panel plots responses for one item. See Table 1 for explanation of the items.

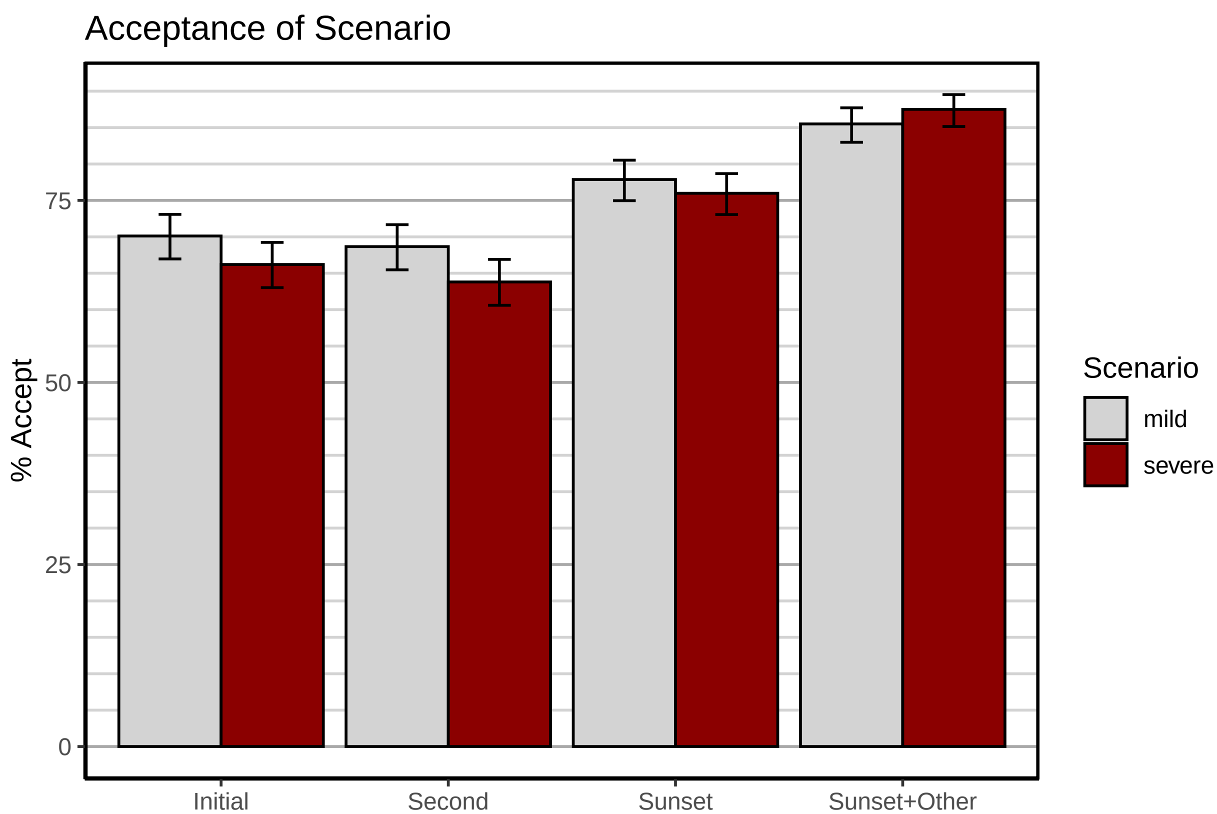

Figure 3. Acceptability of scenarios during the first wave (28-29 March 2020). The 4 pairs of bars refer to the 4 acceptability questions; see Figure 1. Error bars are 95% confidence intervals computed by R function *prop.test*.

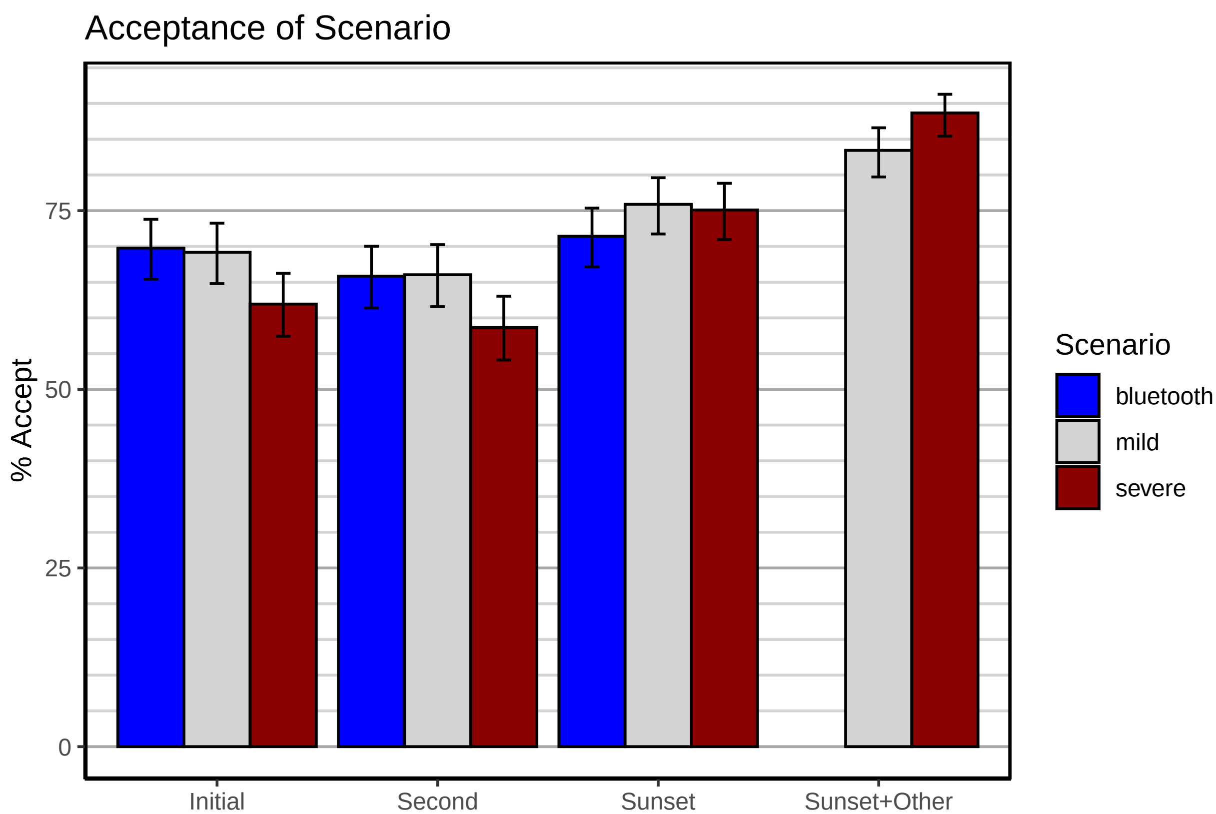

Figure 4. Acceptability of scenarios during the second wave (16 April 2020). The 4 pairs of bars refer to the 4 acceptability questions; see Figure 1. Error bars are 95% confidence intervals computed by R function *prop.test*. Note that the “Sunset + other” question was not presented in the Bluetooth scenario.

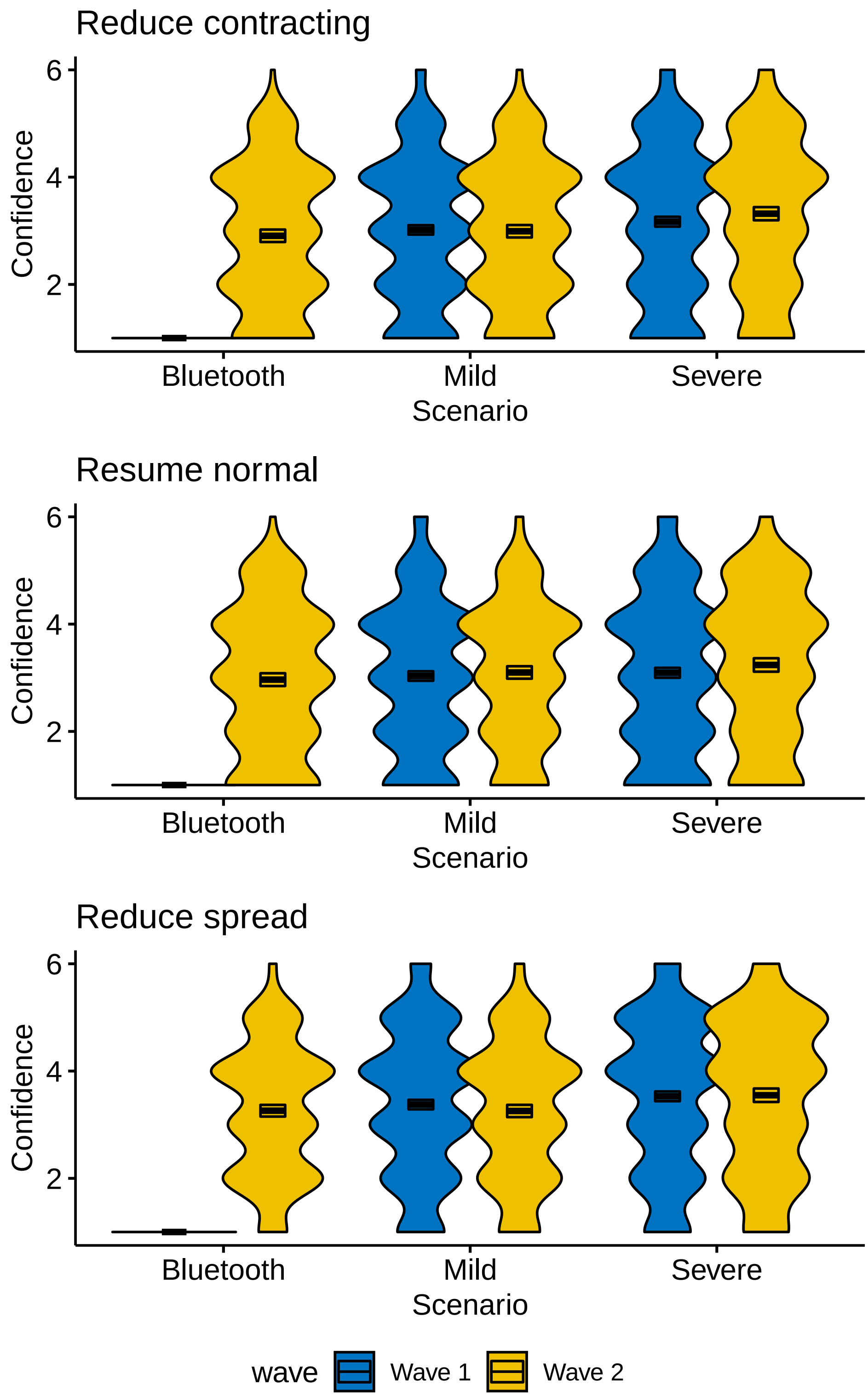

Figure 5. Participants' confidence in the expected benefits from the three tacking policies. Box plots enclose 95% confidence intervals. Panels represent different items, using the labeling from Table 2.

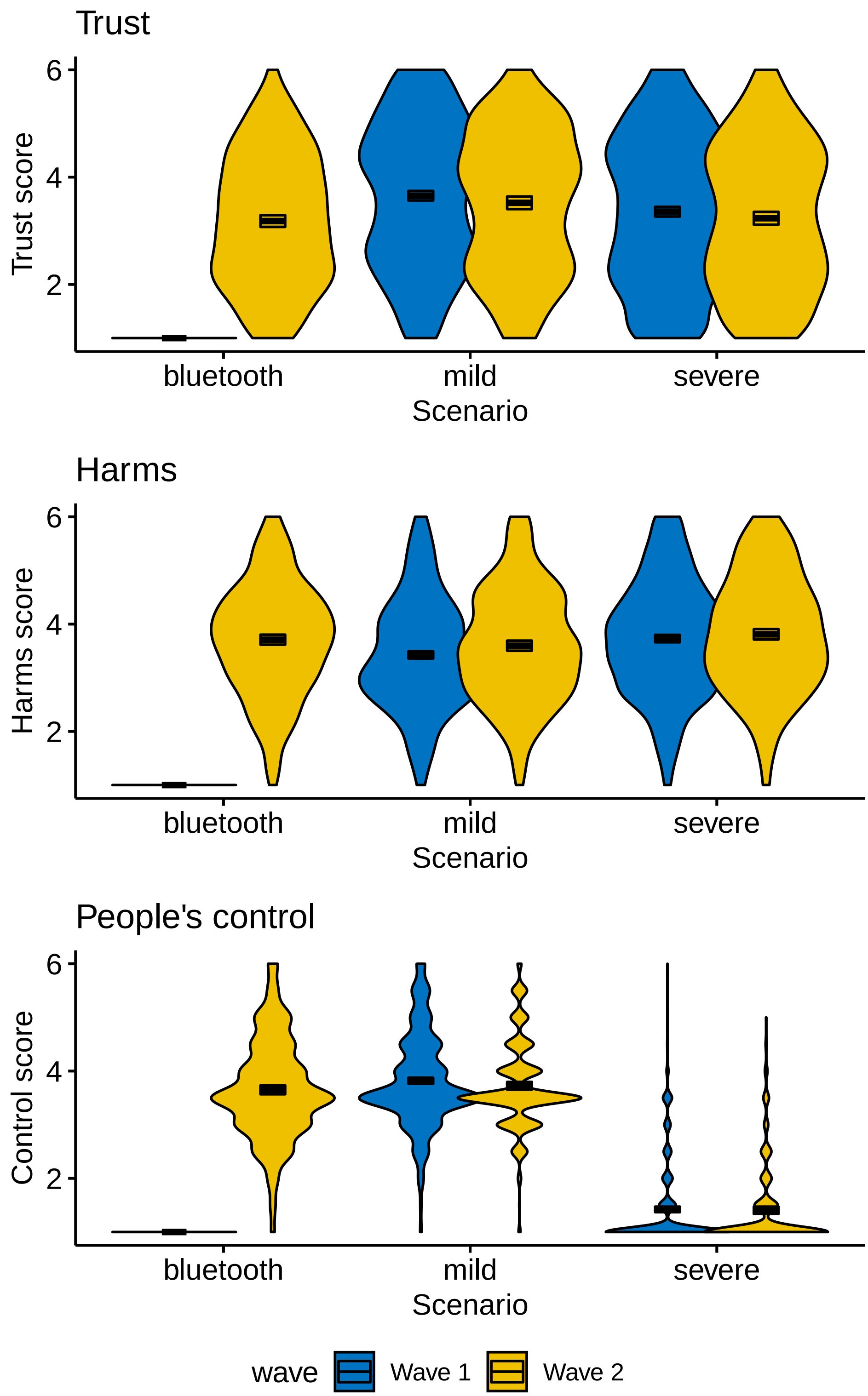

Figure 6. Participants' views on the expected harms and risks of the three tacking policies and perceived trust in the government's intentions. Box plots enclose 95% confidence intervals. Panels represent different item clusters; see text for details.

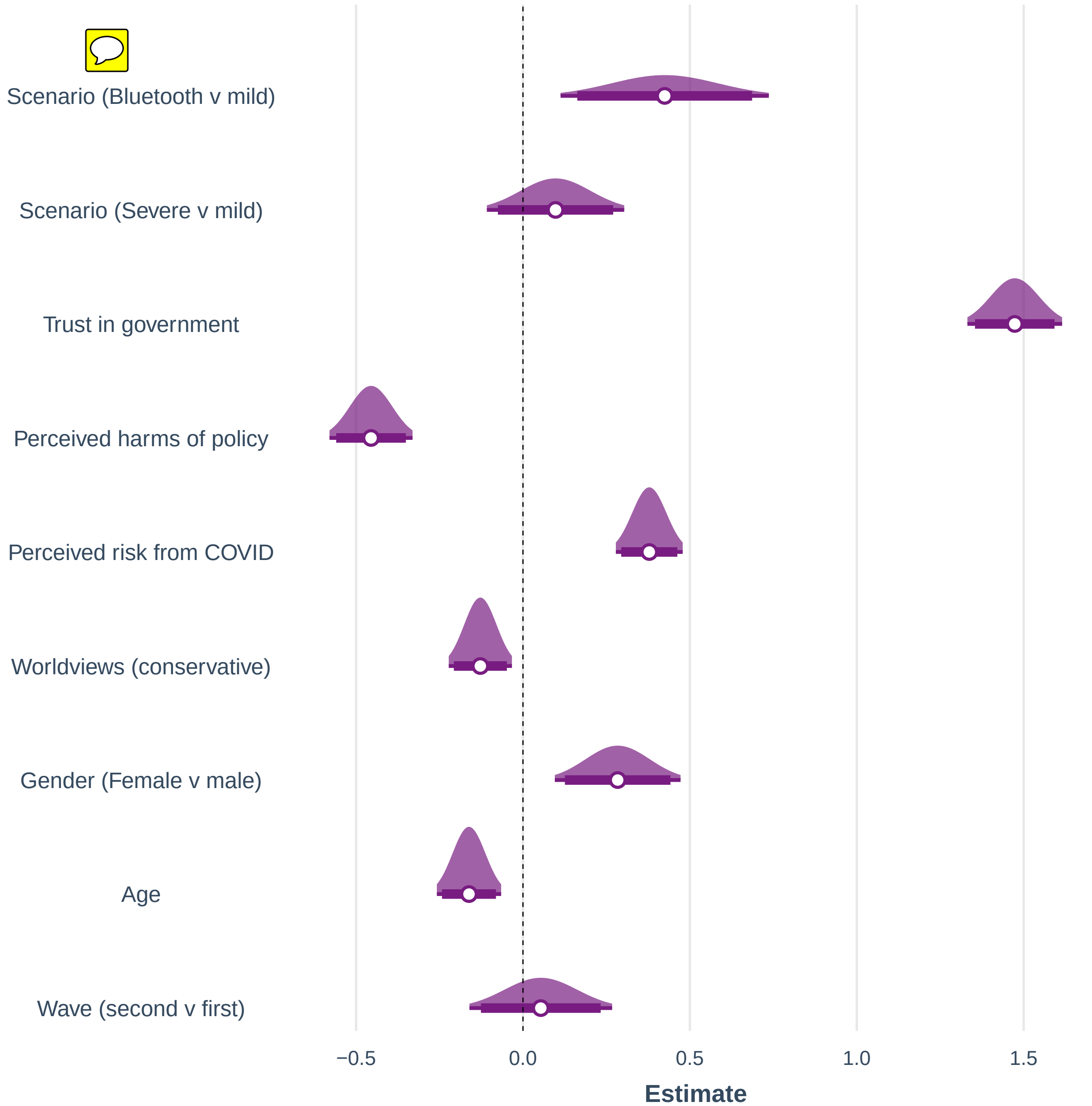

Figure 7. Estimated standardized coefficients for a logistic regression to predict initial policy acceptance. Distributions span 95% confidence intervals. Horizontal bars span 90% confidence intervals.

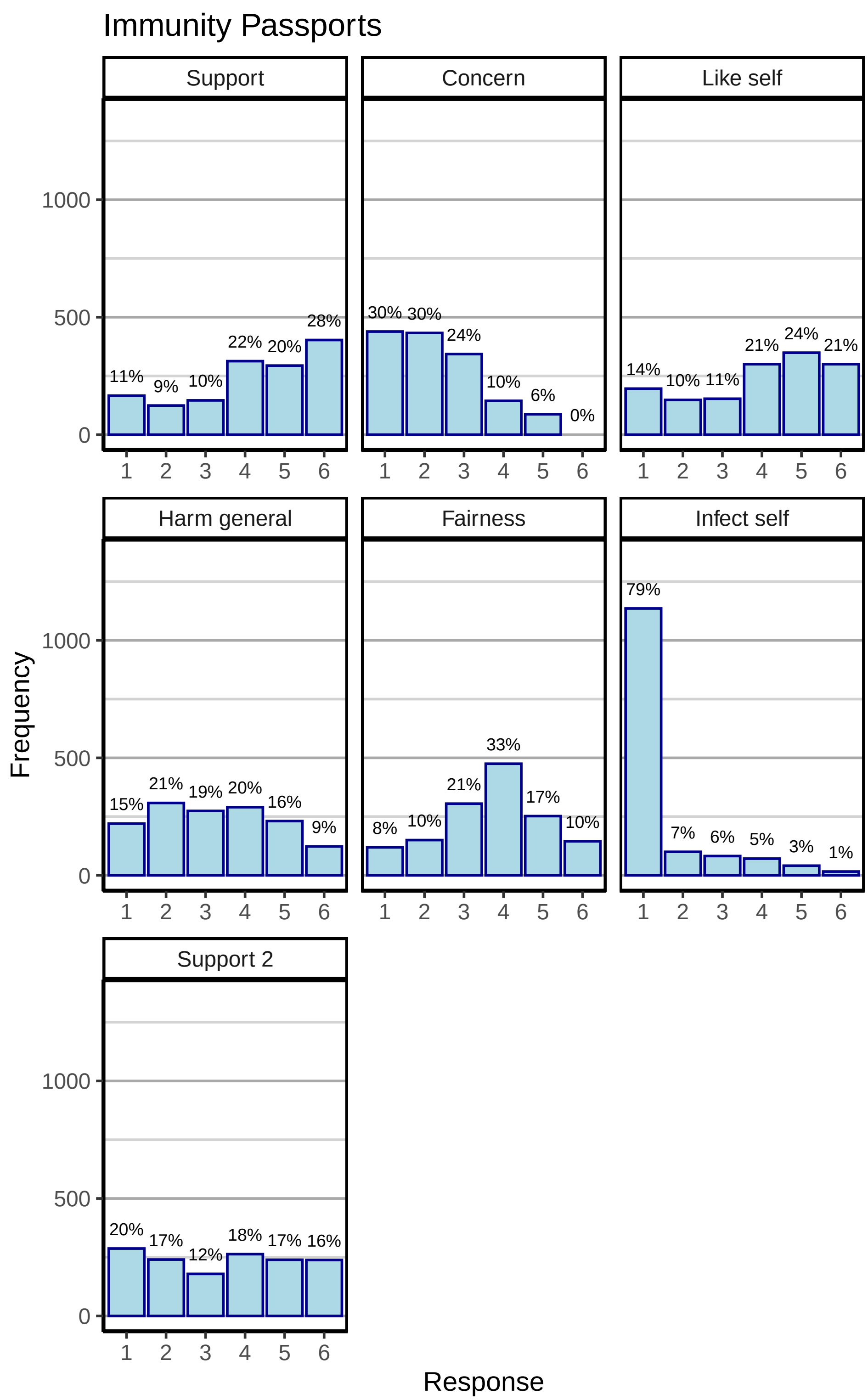

Figure 8. Responses to items concerning immunity passports during wave 2. Each panel plots responses for one item before reverse scoring. See Table 3 for explanation of the items. The "concern" item used a 5-point scale.

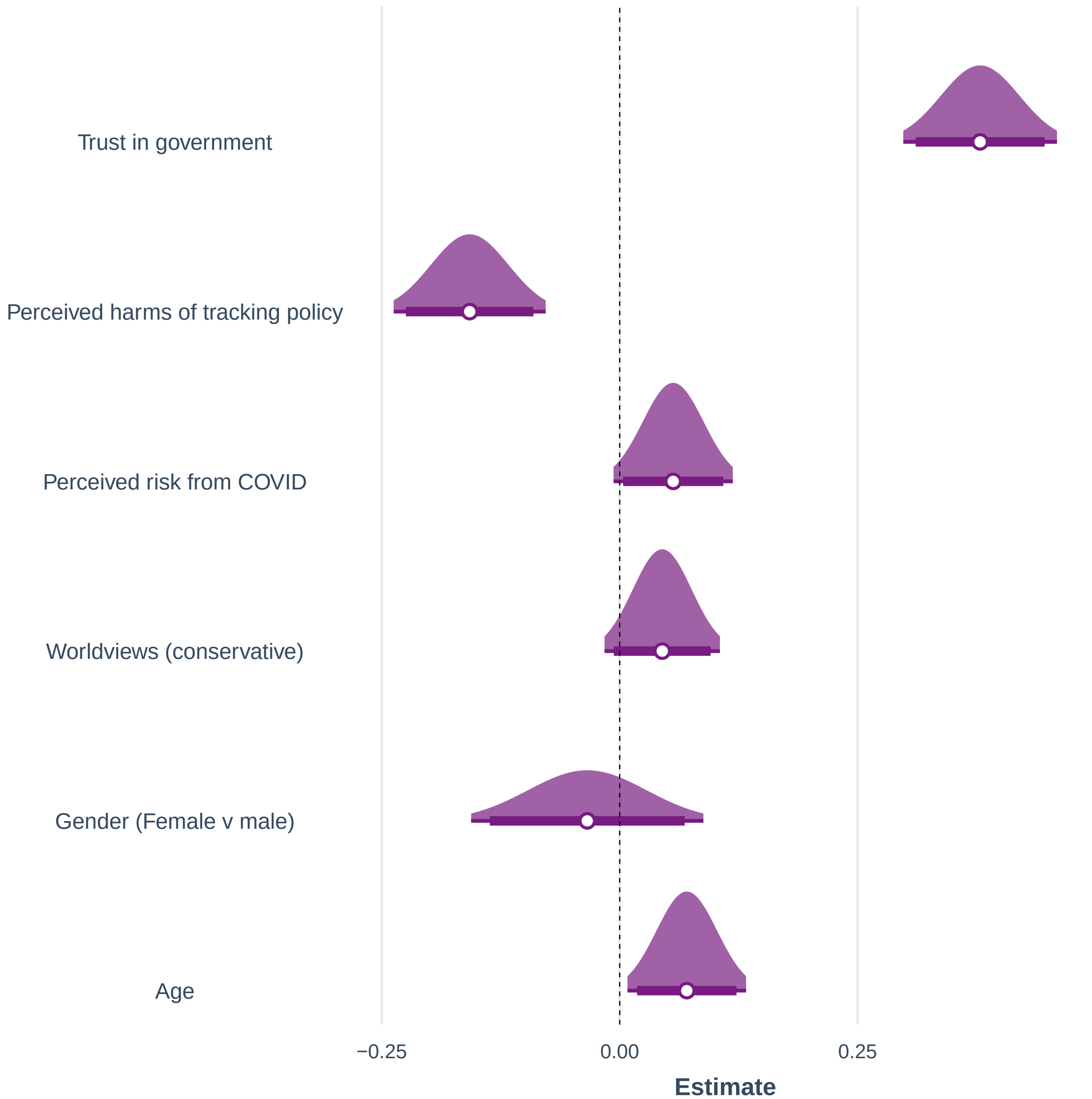

Figure 9. Estimated standardized coefficients for a linear regression to predict favourable attitudes towards immunity passports. Distributions span 95% confidence intervals. Horizontal bars span 90% confidence intervals. Note that Trust in government and Perceived harms are obtained in response to the tracking policy scenario, not immunity passports.