







# Did the GDPR increase trust in data collectors? Evidence from observational and experimental data

Paul C. Bauer <sup>a</sup>, Frederic Gerdon <sup>a</sup>, Florian Keusch <sup>a</sup>, Frauke Kreuter <sup>b,c,d</sup> and David Vannette<sup>e</sup>

<sup>a</sup>University of Mannheim, Mannheim, Germany; <sup>b</sup>University of Maryland, College Park, MD, USA; <sup>c</sup>Institute for Employment Research, Nuremberg, Germany; <sup>d</sup>Ludwig Maximilian University of Munich, Munich, Germany; <sup>e</sup>University of California, Davis, CA, USA

## ABSTRACT

In the wake of the digital revolution and connected technologies, societies store an ever-increasing amount of data on humans, their preferences, and behavior. These modern technologies create a trust challenge, insofar as individuals have to trust data collectors such as private organizations, government institutions, and researchers that their data is not misused. Privacy regulations should increase trust because they provide laws that increase transparency and allow for punishment in cases in which the trustee violates trust. The introduction of the General Data Protection Regulation (GDPR) in May 2018 – a wide-reaching regulation in EU law on data protection and privacy that covers millions of individuals in Europe – provides a unique setting to study the impact of privacy regulation on trust in data collectors. We collected survey panel data in Germany around the implementation date and ran a survey experiment with a GDPR information treatment. Our observational and experimental evidence does not support the hypothesis that the GDPR has positively affected trust. This finding and our discussion of the underlying reasons are relevant for the wider research field of trust, privacy, and big data.

## ARTICLE HISTORY

Received 8 May 2020  
Accepted 16 April 2021


## KEYWORDS

Trust; GDPR; big data; privacy; surveillance; data protection

## Introduction

In the wake of innovations in information and communications technologies (ICTs), commercial and public institutions store an ever-increasing amount of data on humans and their behavior. This stock reaches from data collected via smartphones by location and health tracking applications to data stored during social media use. The opportunities and dangers of this technological advancement are discussed across various disciplines (Anthony et al., 2017; Brayne, 2017; Golder & Macy, 2014; Hacker & Petkova, 2017; Mayer-Schönberger & Cukier, 2012; Nissenbaum, 2009; Watts, 2004) and scholars have described these developments using concepts such as ‘surveillance society’ (Lyon, 2001) or ‘surveillance capitalism’ (Zuboff, 2019).

**CONTACT** Paul C. Bauer  [mail@paulcbauer.eu](mailto:mail@paulcbauer.eu)

 Supplemental data for this article can be accessed at <https://doi.org/10.1080/1369118X.2021.1927138>

© 2021 Informa UK Limited, trading as Taylor & Francis Group

As these developments are potentially intrusive to the privacy of individuals, the questions of how data collectors manage and use the data become crucial. The long-term functioning of these recent technologies in a democratic society requires trust. Individuals who leave data traces either knowingly, for example, by filling out personal and financial information to make an online purchase, or unwittingly because their behavior is recorded through third party cookies or digital fingerprinting, need to be able to trust data collectors that their data is safe and not used to their disadvantage. Trust in the practices of data collectors is not only relevant as a potential determinant of individuals' data-sharing<sup>1</sup> behavior (Bauer et al., 2019), it is also an indicator that reflects to what extent individuals feel comfortable with the data collection practices they encounter in their daily lives by both public and private actors. While scholars recognize the urgency of studying how these technological changes interact with attitudes and behavior, empirical sociological research on this issue is still in its infancy. For instance, empirical sociological research is only starting to identify the implications of ICT for trust in institutions (cf. Anthony et al., 2017, p. 263).

After a slower start, laws are increasingly introduced that protect individuals' digital privacy. On 25 May 2018, the European Union (EU) implemented one of the most wide-reaching policies on data protection – the General Data Protection Regulation (GDPR) – with the goal to clarify, codify, and extend individuals data rights.<sup>2</sup> The European Commission stated that several civil rights and consumer organizations understood the GDPR 'as an important contribution to a fair digital society built on mutual trust' (European Commission, 2019a, p. 7) and companies reported that it represented an opportunity to build trust with commercial partners and customers alike (ibid., p.8). Thereby, the GDPR aims to regulate the topical challenge of preserving the rights of information and privacy while not excessively hindering business performance. The effects on how companies handled and stored data, along with how they interacted with users, were immediately visible. For instance, companies such as Google increasingly stored data of European users in Europe as to comply with the corresponding provisions (Lindsey, 2019; O'Brien, 2018). The impact of this policy reaches beyond the borders of the EU and pundits suggest that other countries should follow suit (Faitelson, 2017; Goddard, 2017; Rubinstein & Petkova, 2018; The Economist, 2018). Against this background, our study focuses on the impact of this wide-reaching regulation on trust and specifically seeks to address the following question: *Does the EU General Data Protection Regulation (GDPR) affect individuals' trust in data collectors?*

To study GDPR's effects on trust, we combine a longitudinal with an experimental approach. We collected panel data on individual's perceptions and trust before and after the implementation of the policy on 25 May 2018. Moreover, we conducted a survey experiment in which we randomly treat individuals with information about the content of the GDPR policy and subsequently measure their trust in a number of entities. In addition, we provide descriptive statistics of how awareness of the GDPR and related attitudes changed over the course of 2018.

With this study, we contribute to the existing scholarship in several ways. First, current empirical research focuses on the interaction of norms and expectations in the sphere of privacy (Horne & Przepiorka, 2019), on the link between perceptions, expectations, and data-sharing behavior (Bauer et al., 2019; Michaelidou & Micevski, 2019), on the transformation of surveillance practices through ICTs and big data analytics

(Brayne, 2017), and on the role of individual characteristics and the situations for trust in data collectors such as physicians (Campos-Castillo & Anthony, 2019). Regulatory frameworks provide rules and orientation for those who receive, as well as those who give data. Therefore, the implementation of a framework such as the GDPR may affect people's behaviors and their normative expectations. However, we lack empirical research that confirms or refutes such an effect. In the present study, we examine whether a change in regulations (introduced and sanctioned by a third party) affects individuals' expectations, namely their trust in data collectors.

Second, our study is the first to explore the consequences of one of the most far-reaching policies of the twenty-first century on individuals' attitudes. So far, research focusing on the GDPR has been concerned with its legal ramifications and its impact on the economy and businesses (Allen et al., 2018; Baker, 2017; Barnard-Wills et al., 2016; Bieker et al., 2016; Binns, 2017; Ciriani, 2015; Morrissey, 2016; Tankard, 2016; van Ooijen & Vrabec, 2018). However, apart from Presthus and Sørsum (2018), which investigated awareness and perception of the GDPR in a small online survey in Norway ( $N = 200$ ), we know next to nothing about how this EU-wide policy affected the attitudes of its actual beneficiaries<sup>3</sup>: the individuals whose data rights were clarified, codified, and extended. It is those same individuals who will or will not provide fuel for the data economy of the twenty-first century.<sup>4</sup>

Third, our study is innovative from a methodological point of view as we approach the question from a causal perspective, which is a challenge identified in the wider policy feedback literature (Campbell, 2012, p. 343). To this end, we combine longitudinal survey data with experimental data that were both collected for the purpose of this study. In addition, we rely on a set of trust measures that measure specific trust as opposed to the more general, but also more vague scales that have been used to measure generalized trust and privacy concern in past research. We proceed as follows: Section 2 develops our hypothesis and discusses the process through which GDPR awareness should impact trust. Section 3 presents the design, data, and measures. Section 4 summarizes the results. Section 5 provides a conclusion, discusses limitations, and provides rationales for future research.

## Theory: the GDPR and trust in data collectors

Trust is invariably linked to questions of privacy and data (Anthony et al., 2017) and sharing data creates a problem of trust (Seligman, 2000). Individuals make themselves vulnerable when disclosing personal information because this information could be used for an unintended and harmful purpose – either by the primary data collector or through third parties (Anthony et al., 2017; Nippert-Eng, 2010; Petronio, 2002; Richardson, 1988). For instance, it is by now well-known that geolocation data can and have been used to deanonymize and track individuals as well as that there is an illicit market for such data (de Montjoye et al., 2013; Freudiger et al., 2012; Thompson & Warzel, 2019).

We conceptualize a trust relationship as follows. A trust relationship entails a trustor A who has an expectation regarding a trustee B regarding some behavior X in situation or context Y at time  $t$  (Bauer, *forthcoming*; Bauer & Freitag, 2018, p. 2). In the context of privacy and data collection the trustors are individuals (A) and the trustees (B) are data collectors. In such situations individuals would normally expect organizations to

keep their data safe and not use it to their disadvantage (X). Such expectations should be governed by context-specific privacy norms, that is, what is perceived to be an appropriate data practice for a given scenario (Martin & Nissenbaum, 2017; Martin & Shilton, 2016a, 2016b; Nissenbaum, 2004, 2018).

Only if individuals are aware of data collection, can trust have an effect on their behavior. Individuals knowingly share their data in many situations. For instance, we would assume that most users of Google Maps know they are sharing their geolocation. However, in other situations, they may do so unwittingly, for instance the very same smartphone users may not be aware of the fact that other apps also access their geolocation.

Let us illustrate the relationship between trust and awareness with two examples. In one scenario (1), an individual A uses an application, for example, a smartphone app, is aware of the data the app collects and has an expectation of how the data collector handles the data. For instance, A could trust this data collector; otherwise, A would not install the app in the first place (Bauer et al., 2019). However, once A shared data and the data collector acts against A's expectation, A will feel betrayed. In another scenario (2), individual A is not even aware that the application collects personal information and therefore does not have any expectations regarding the data collector's behavior. In this situation, the expectation (i.e., trust) plays no role in the data-sharing decision as there is no awareness that any data is being shared. Nonetheless, if it becomes known later that the data collector has passed on the data, A could – despite having no expectations initially – still feel cheated and perceive the data collector's behavior as a betrayal – which in turn should affect future trust. When organizations collect data, they can prove their trustworthiness, which may result in an increase in trust over time, but it also creates the opportunity to lose individuals' trust (Petronio, 2002). As Baier (1986, p. 242) writes: '[t]rust is much easier to maintain than it is to get started and is never hard to destroy.'

As we propose for the context of the GDPR and data protection, the relationship between truster and trustee is often mediated by third parties. If such third parties enforce trustees' trustworthy behavior it may also affect the truster and increase her trust (Burt & Knez, 1995; Buskens et al., 2010; Wang & Ng, 2015). If A is aware of a third actor C that enforces that B really displays A's preferred behavior X, then A's trust, that is A's expectation that B really will display behavior X, should be strengthened. For instance, if A is considering sharing her data with B, knowing that there is an actor C that both clearly defines what is expected of B and that also enforces that B behaves in this way should increase A's trust in B.<sup>5</sup>

The state and its laws can represent such a third-party C that enforces data collectors' trustworthy behavior on behalf of the truster. A recent example is the fine Facebook was subjected to by the U.S. Federal Trade Commission for mishandling users' personal information (Feiner, 2019; Kang, 2019). While this is a high-profile case, it is not the only one (Liu et al., 2015; Peretti, 2008). In principle, knowing that organizations can be and are held accountable when they are careless or misuse individuals' data should make them more trustworthy and increase individuals' trust.

In this regard, the GDPR has fundamentally altered the relationship between individuals and data collectors as well as the state's role as a third party. The GDPR has been in effect since May 2018 and aims at codifying and enforcing better data protection rights for European citizens. Importantly, it strongly expands existing and introduces new

rights for individuals. Among others, the GDPR awards individuals with the following rights (EU General Data Protection Regulation, 2016):

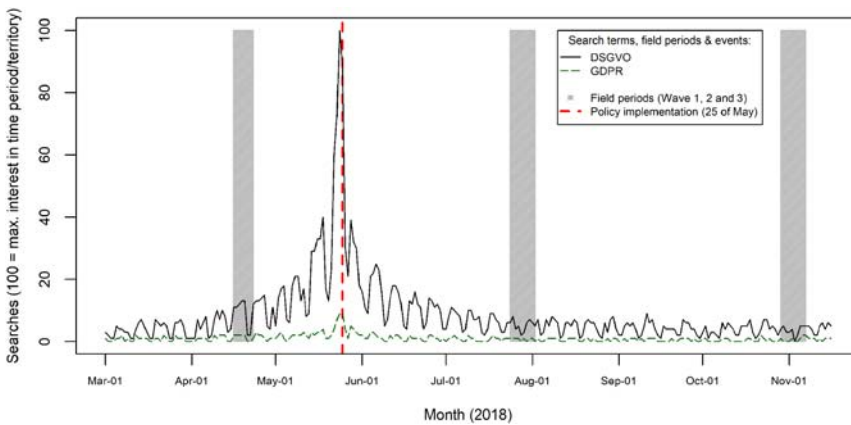
The right to clear and comprehensible information about who is processing your data, which data is being processed and why; Right of access to the personal data that an organization has about you; Right to ask a service provider to transfer your personal data to another service provider, e.g., if you switch to another social network on the Internet; Right to be “forgotten”, i.e., to have your data deleted if you no longer wish it to be processed and if there are no legitimate reasons for the company concerned to continue storing the data; Companies that want to process your data must ask for your consent and clearly state how they want your personal data to be used; If your data is lost or stolen, the company responsible must immediately notify you and the appropriate data protection authority if this breach threatens to harm you.

In short, the GDPR clearly defines the behavior that individuals can expect of data collectors. It changes individuals’ leverage in terms of how much control and knowledge they (can) have about the data that is stored and used. It also increases state institutions’ power to sanction data collectors that disregard those rights on behalf of individuals.<sup>6</sup> Actors that violate the GDPR face fines of up to 4% of their global annual revenues (Greengard, 2018). If individuals become aware of the GDPR policy and relatedly the rights it bestows upon them, it should increase individuals’ trust because individuals can now expect to a higher degree that data collectors will not misuse their data. Importantly, the GDPR policy is extraordinarily complex, and we cannot assume that individuals grasp all its details. However, for the mechanism described to take effect, it is merely necessary that citizens are aware of the policy’s implementation and of its aim, namely to protect them in their relation to data collectors. Below we will comment on how we identify whether individuals in our study are aware of the GDPR and its contents.

In sum, we would expect that awareness of the GDPR has a positive effect on individuals’ trust in data collectors (H1). While it is not the primary focus of our study, we would also expect that concrete, situational trust judgments that focus on a particular trustee (e.g., a data collector) and behavior by this trustee may be influenced by generalized trust as well as privacy concern. In our empirical analysis we also measure and account for these latter characteristics.

## Methodology: data, measures, and methods

In 2018, we conducted three web surveys among members of the German non-probability online panel Mingle, operated by Respondi AG (<https://www.respondi.com/>). Participants were recruited via email, and we used quotas for gender, age, and smartphone ownership based on the known distribution of these characteristics in Germany (see Table A1 – A4-B for statistics on our sample). The field periods for the surveys were 16–23 April, 2018 (Wave 1), 24 July to 2 August, 2018 (Wave 2), and 29 October to 7 November, 2018 (Wave 3). [Figure 1](#) displays the field periods and Google search trends for the terms ‘DSGVO’ (the German acronym for) and ‘GDPR’ before and after these time periods.<sup>7</sup> The frequency of searches for these terms indicates the salience of the GDPR and therefore may be related to public awareness of the regulation. The graph reflects the increase in interest in the run up to the implementation of the regulation on 25 May, 2018 (see [Figure 1](#)).



**Figure 1.** Time periods of data collection.

Note: Y-axis shows the prevalence of searches relative to each other during the depicted time and in the territory of Germany. Periods of data collection as gray polygons. Lines represent trends of search terms on Google. Searches for ‘Datenschutzgrundverordnung’ and ‘General Data Protection Regulation’ not shown here because they were far less common.

As shown in Figure A3 in the appendix, we used a split-panel design where parts of our sample from Wave 1 were re-interviewed in Waves 2 and 3, and fresh respondents were added for each wave. In Wave 1, 2093 respondents completed the entire questionnaire. In Wave 2, 2043 respondents completed the questionnaire, 482 of which were fresh respondents. In Wave 3, 2112 respondents completed the questionnaire out of which 843 were fresh respondents.<sup>8</sup> Summary statistics for sociodemographics of respondents in all three waves can be found in Tables A2-A – A4-B in the Appendix. The median response time for the three waves were 4 min 21 sec, 4 min 1 sec, and 4 min 22 sec, respectively, and respondents who completed a questionnaire were incentivized with panel points (equivalent to 25 cents per wave) in accordance with the online panel provider’s policy. The questionnaires were programed in Questback EFS Survey Suite (Keusch, 2019).

To answer our research question, we use both observational data from our three-wave panel survey and experimental data from a survey experiment in Wave 3. First, we exploit the fact that we observe individuals on three occasions, once before the implementation of the GDPR and twice afterwards. In all three waves, the same set of six questions was asked:

- Trust in data collectors (end-labeled, 11-point rating scale):<sup>9</sup>
  - ‘On a scale from 0 “not at all” to 10 “completely”, how much do you trust that *Google* uses your personal data only internally, so does not share them with third parties?’
  - ‘On a scale from 0 “not at all” to 10 “completely”, how much do you trust that *Facebook* uses your personal data only internally, so does not share them with third parties?’
  - ‘On a scale from 0 “not at all” to 10 “completely”, how much do you trust that the *Federal Statistical Office* uses your personal data only internally, so does not share them with third parties?’
  - ‘On a scale from 0 “not at all” to 10 “completely”, how much do you trust that *university researchers* use your personal data only internally, so does not share them with third parties?’



- GDPR awareness:
  - ‘Have you ever heard of the EU General Data Protection Regulation 2018?’ (dichotomous response options: Yes, No)
  - [If ‘Yes’] ‘In your own words, what do you think are the objectives of the EU General Data Protection Regulation?’ (open-ended response field)

From the two GDPR awareness questions we constructed a dummy variable that is 1 if respondents indicate that they have heard of the GDPR and if they provide an open-ended response that signals that they are aware of the general aims of the GDPR, and 0 otherwise.<sup>10</sup> In other words, as is required by the mechanism we discussed, our measure identifies people that are not only aware of GDPR but also aware of its fundamental aims reflects the assumptions regarding awareness made in the theory. The trust questions are investigated as four separate outcome variables (see Table A8 for further survey measures).

We model the influence of GDPR awareness on trust in data collectors as follows:<sup>11</sup> First, we estimate models that include only respondents from the cross-sectional dataset from Wave 1 before the GDPR became into effect (see Figure 4 and Table A5), and regress trust in data collectors ( $y$ ) on GDPR awareness ( $D$ ) using the following model:

$$y_i = \beta_0 + \beta_1 D_i + \varepsilon_i \quad (1)$$

where  $y_i$  is individual  $i$ 's level of trust in Wave 1 and  $D_i$  is a dummy indicating whether  $i$  indicated having heard of the GDPR,  $\beta_0$  is the intercept, namely the average trust in the control group, and  $\beta_1$  is the difference in the average trust between the treatment and control groups. In additional models we control for gender, age, education, general privacy concern, Facebook and Google account ownership, device ownership,<sup>12</sup> and generalized trust, as these could be regarded as potential confounders.

Second, we use a difference-in-differences (DID) approach to approximate the causal effect of GDPR awareness on trust in data collectors (Angrist & Pischke, 2008; Croissant & Millo, 2008). Here, we exploit the fact that only a part of our sample became aware of the GDPR in the period between Wave 1 and 2 of our survey. We use the following linear model (see Figure 5 and Table A6):

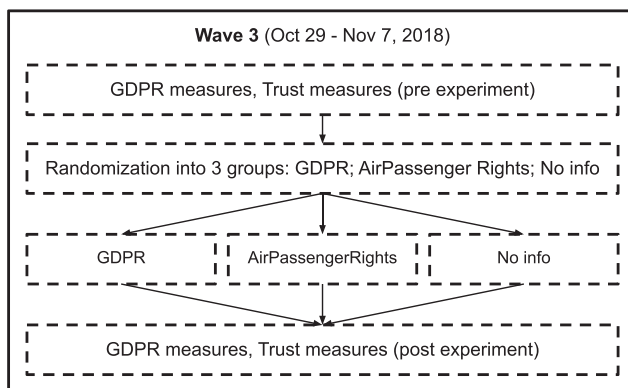
$$\Delta y_i = y_{it-1} - y_{it} = \beta_0 + \beta_1 D_i + \varepsilon_i, \quad t = 1, 2 \quad (2)$$

where  $\Delta y_i$  represents the change in trust in a data collector between Wave 2 and Wave 1 for individual  $i$ ,  $D_i$  is a dummy indicating whether someone became aware of the GDPR between W1 and W2,  $\beta_1$  is the difference in the average change between the treatment and control groups. We only focus on two time periods – Wave 1 and 2 – in this second step as the event we are interested in – the implementation of the GDPR – happened between these two time points. As we analyze panel data from two waves, we exploit variation between individuals rather than within individuals. The estimated coefficient represents the difference in the average trust change between individuals who *heard of the GDPR* and individuals who did not between Wave 1 and Wave 2. In further models, we add control variables measured at  $t_1$  to the equation.

In our analysis of the panel data, we excluded respondents who indicated having heard of the GDPR in Wave 1 and *not* having heard of the GDPR in Wave 2 (87 respondents). We also excluded respondents who indicated having heard of the GDPR in both Wave 1 and 2 (274 respondents). Accordingly, our ‘treatment’ groups consist of respondents who indicate having *not* heard of GDPR in Wave 1 and having heard of GDPR in Wave 2 (475 respondents) and our comparison/control group consists of respondents who indicate having *not* heard of GDPR in Wave 1 and having *not* heard of GDPR in Wave 2 (725 respondents).

Regarding causality, we rely on a difference-in-differences logic. We estimate trends in two groups and assume that the trend in the treatment group would mirror the trend in the control group given the treated units had not become aware of the GDPR and vice versa (*parallel trends assumption*). Once controls are added, one assumes parallel trends conditional on these controls (conditional parallel trends assumption). Unobserved time-varying confounders would threaten this assumption. This would be the case, for instance, if many individuals in the treatment group (and not the control group) were systematically exposed to a media report that both causes them to inform themselves about the GDPR as well as affects their trust. But we think that this is unlikely here. The controls we add are gender, age (categorical), education (categorical), privacy concern, accounts of different platforms (as dummies), possession of different devices (as dummies) and generalized trust.<sup>13</sup>

As an even more solid test of causality, we also implemented an experiment in Wave 3 of our panel study (see Figure 2). We first asked all Wave 3 respondents ( $n=2112$ ) the questions about trust in four data collectors. We then randomly treated 50% of the respondents with information about the GDPR, 25% with information about air passenger rights, and 25% with no information (see Figure A2). We then asked all respondents about their trust in two data collectors (Facebook, Google), using the same questions as before. The advantage is, first, that we are in control of treatment assignment as opposed to the treatment variable in our panel data into which respondents may self-select (GDPR awareness) and, second, that we know exactly what kind of information we gave to the respondents. As comprehension of the given treatment is a prerequisite for its potential effectiveness, we also asked respondents about how comprehensible they assessed the text



**Figure 2.** Flow chart of the survey experiment.



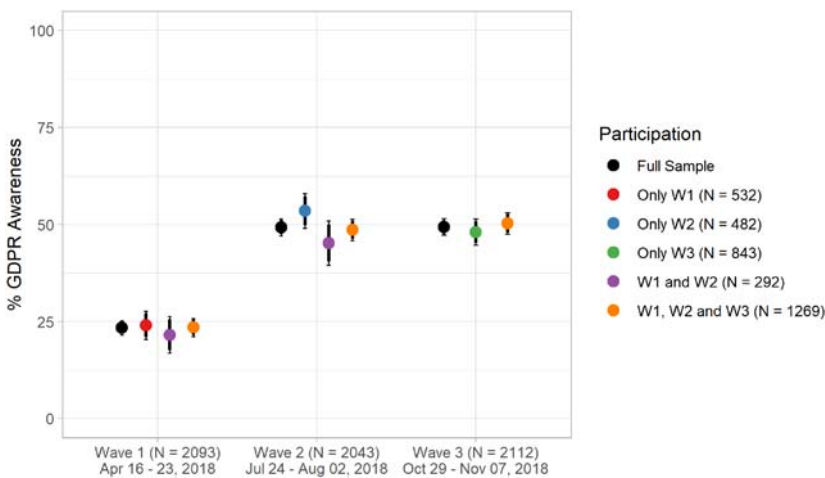
(from 1 = 'not comprehensible at all' to 4 = 'very comprehensible') and include this variable in our analysis.

While we acknowledge that our sample is non-probabilistic in nature and we thus have to be careful when inferring point estimates for the entire German population (Kohler, 2019), we are confident that the modeling approach using the panel data and the experimental approach allow us to produce unbiased causal estimates. (Figure 3).

## Empirical results

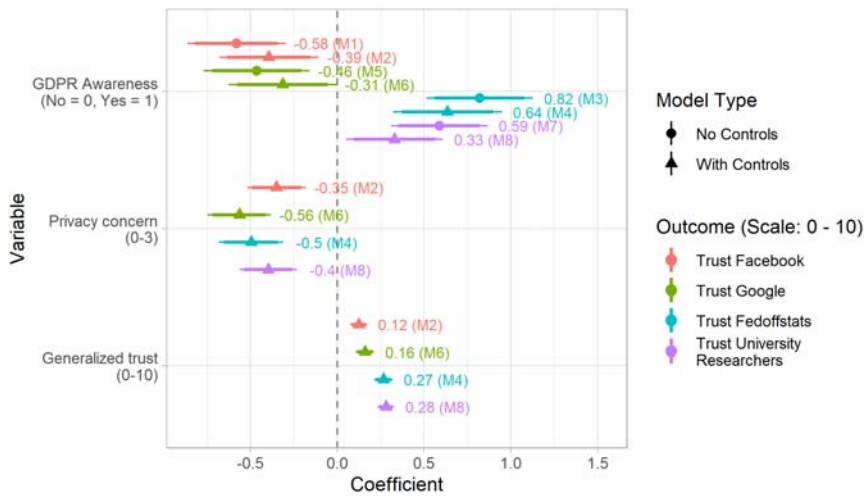
We start with a few descriptive statistics on both our treatment variable and our outcome variables. Figure 4 displays the percentage of respondents who reported having heard of the GDPR across our three waves. The graph depicts percentages for the full sample for each wave (black point), but also for different subsets such as respondents who only participated in Wave 2. As expected, the proportion of respondents aware of the GDPR increases from around 23 percent before the implementation of the GDPR (Wave 1) to around 49 percent after the policy was implemented (Wave 2). Thereafter, from Wave 2 to 3, the proportion of respondents being aware of the GDPR remains relatively stable. Figure 4 also allows us to compare respondents who participated in all three waves to respondents who joined in Wave 2 or 3. One concern was that participation in Wave 1 may cause respondents to look up information on the GDPR. In other words, confronting them with our awareness question in Wave 1 could have artificially increased awareness in subsequent waves. However, this does not seem to be the case since respondents who joined in Wave 2 have similar awareness levels as those who already participated in Wave 1. Awareness does not seem to be influenced by being part of the panel study.<sup>14</sup>

Figure A4 in the appendix displays the means of trust across the three waves for the full samples of the respective waves. Among those surveyed, there is a slight increase in trust during this time.



**Figure 3.** GDPR Awareness across 3 waves.

Note: Respondents who participated only in W2 and W3 ( $N = 3$ ) and only in W1 and W3 ( $N = 2$ ) were omitted in this graph. Black bars represent 90% (thick) and 95% (thin) confidence intervals.

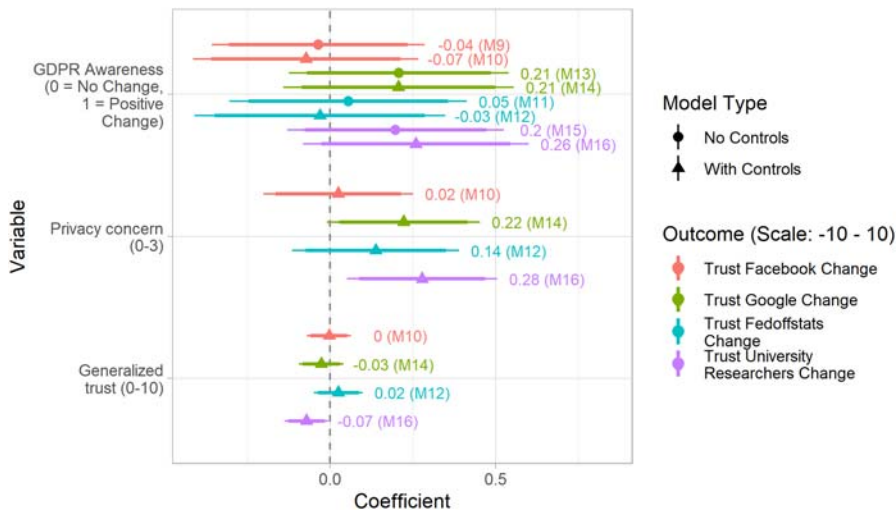


**Figure 4.** Linear model predicting trust in four data collectors in Wave 1.

Note: Graph only displays coefficients for the main independent variable (GDPR awareness) and the most important control variables (general privacy concern, generalized trust). Estimates for socio-demographics (sex, age, education), Facebook and Google account, and device ownership have been omitted but can be found in Table A5. Bars represent 90% (thick) and 95% (thin) confidence intervals.

We investigate our question about the influence of GDPR awareness on trust in data collectors both with *panel data* and with a *survey experiment*. In Figure 4 (see Table A5) we start with models estimated based on Wave 1 respondents. The outcome variables are the responses to the four trust questions. Rather than to approximate the causal effect, these models serve to provide a first estimate of the difference between our two groups, namely respondents aware of the GDPR and respondents not aware of it. The coefficients at the top describe the difference in the trust means across respondents who indicated having heard of the GDPR and respondents who reported not having heard of the GDPR before the introduction of the policy. Figure 4 (cf. Table A5) reports both bivariate effects (M1, M3, M5, M7; estimates indicated by a dot in the figure) and effects controlling for a set of covariates (M2, M4, M6, M8; estimates indicated by a triangle in the figure). We find statistically and substantively significant differences without and with controls. Respondents who have heard about the GDPR have on average lower trust in Google and Facebook and higher trust in the Federal Statistical Office as well as university researchers. The effects sizes range between  $-0.58$  and  $0.82$  in the uncontrolled models and between  $-0.39$  and  $0.64$  in the controlled models, which is substantial on the 11-point trust scales. In Figure 4 we also added two more, theoretically relevant covariates (a subset), that are strongly related to trust not only conceptually. As one would expect we find negative effects for privacy concern and positive effects for generalized trust on trust in all four data collectors.

Figure 5 (cf. Table A6) visualizes the results of the linear model based on panel data from Wave 1 and 2 (see Eq. 2). The outcome variables are now the change in trust between  $t_1$  and  $t_2$ . The intercepts in the bivariate models (M9, M11, M13, M15; estimates indicated by a dot in the figure) represent the average change in the control group (GDPR Awareness = 0), the GDPR coefficients in those models represent the difference in the



**Figure 5.** Linear model predicting changes in trust in four data collectors between Wave 1 and Wave 2.

Note: Graph only displays coefficients for the main independent variable (change in GDPR awareness) and the most important control variables (general privacy concern, generalized trust). Estimates for socio-demographics (sex, age, education), Facebook and Google account, and device ownership have been omitted but can be found in Table A6. Bars represent 90% (thick) and 95% (thin) confidence intervals.

trend between the treatment group (those became aware of the GDPR between W1 and W2) and the control group (those who were aware of the GDPR in W1 and W2). Again [Figure 5](#) also displays a subset of the covariates of the multivariate models (M10, M12, M14, M16; estimates indicated by a triangle in the figure).

The models in [Figure 5](#) (cf. Table A6) indicate that there are no significant differences in the trust trend between respondents who have learned of the GDPR between Wave 1 and 2 and respondents who have not. The maximum difference in the multivariate models was found for trust in university researchers, where respondents who became aware of the GDPR display an even more positive trend than the respondents in our ‘control’ group. However, given that individual changes of less than .5 on the underlying trust scales may range from -10 to 10, these differences in average trends seem rather low.

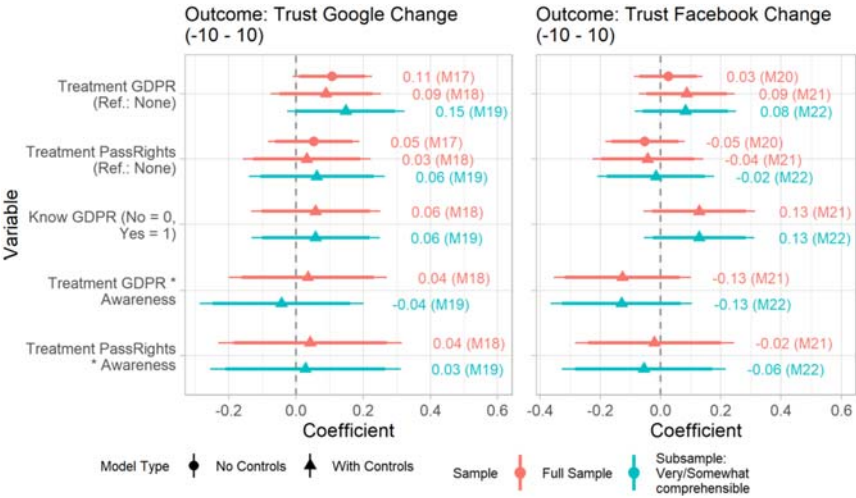
One potential explanation for the small and insignificant effects could be that there are ceiling effects. Respondents who already display high levels of trust before they become aware of the GDPR are less likely to be affected. However, additional estimations (not shown here, available upon request) in which we only included respondents with low trust levels at Wave 1 (max. trust value across all trust scales of 5) provide no evidence in this regard.

Figure A1 in the appendix visualizes the distribution of changes on the outcome variables and the GDPR variable between Wave 1 and 2 for the balanced panel sample of Wave 1 and Wave 2. It indicates that trust in different organizations has remained stable for most respondents in our panel.

In our view, the fact that we see significant differences in the models based on cross-sectional data ([Figure 4](#), M1 – M8, Wave 1, Outcome: Trust) as opposed to the models

based on panel data (Figure 5, M9 – M16, Wave 1, Outcome: Trust Change) can be explained by selection effects in the former that are due to unobserved stable confounders. While we control for various characteristics (age, education, privacy concern, generalized trust, etc.) it is possible that individuals select into GDPR awareness based on a stable attribute of political interest or news consumption. If these individuals in turn are also better informed about various data scandals, it would explain why we see differences in the cross-sectional data but not when canceling out stable characteristics in our panel data models. From a causal perspective the panel data models represent the stronger test and they do not yield evidence for H1.<sup>15</sup>

As an additional test of our hypothesis, we ran an experiment in which we tested whether information on the GDPR could increase trust in Google and Facebook. Figure 6 (Table A7) provides the results of our experiment (M17, M18, M19, M20, M21, M22). The outcome variable is the change in trust in Google (left panel) and Facebook (right panel) measured right before the experimental treatment and directly thereafter. For instance, the top-left coefficient in Figure 6 describes the difference in the average change between those that were treated with GDPR information and those that were not treated with any information. Figure 6 visualizes Model 17 (Google) and 20 (Facebook) that only include the experimental treatment variable as a factor (the baseline is no information), Model 18 (Google) and 21 (Facebook) that add controls, and finally, Model 19 (Google) and 22 (Facebook) that include controls and reduce the sample to those respondents who reported that the GDPR information is comprehensible. We find that there is no effect of our experimental treatment – information on the GDPR – mirroring the findings from the observational data.



**Figure 6.** Linear model predicting change in trust before and after the experimental treatment (GDPR information).

Note: Graph only displays coefficients for the experimental variable that was coded as a factor (Treatment: GDPR; Treatment: air passenger rights), as well as coefficients for one additional covariates namely 'Knowing the GDPR' and the interaction effects of this covariate with the treatment variable (coded as a factor). The corresponding estimates can be found in Table A7. Bars represent 90% (thick) and 95% (thin) confidence intervals.

## Conclusion

*Does the EU General Data Protection Regulation (GDPR) affect individuals' trust in data collectors?* In principle, far-reaching policies that ought to protect individuals' data and hold data collectors accountable should fundamentally change the trust relationship in this sphere. Since the GDPR is a far-reaching policy that concerns millions of individuals, it has triggered widespread media discussion around its implementation in 2018. Around this time, general interest also spiked in Germany as indicated by searches on Google (see [Figure 1](#)). The implementation of a fundamental policy, gaining such wide public attention represents a unique opportunity to test how regulations affect expectations within the realm of surveillance and privacy.

We expected that individuals' trust in data collectors would increase because of the policy, which was our motivation for data collection in the first place. Against our expectations we do not find an effect both relying on our panel survey and a survey experiment based on German samples. Importantly, the two methods make use of slightly different operationalizations of GDPR awareness. While the GDPR treatment variable in the panel survey reflects awareness and knowledge of GDPR's basic aim, the GDPR treatment in our survey experiment provides participants with more extensive information. Hence, we are relatively certain that the non-finding is not related to the treatment. Similarly, our trust measures are more specific as compared to other standard measures of trust (Bauer & Freitag, 2018).

The fact that we do not find an effect could reflect that there really is none. First, although we did check respondents' understanding of the GDPR's content broadly, many people might not be fully aware of its exact stipulations. Numerous studies suggest that people have trouble reading, understanding, and comprehending privacy policies and informed consent paperwork (e.g., Bashir et al., 2015; McDonald & Cranor, 2008). Potentially the same is true for the GDPR. Second, it is possible that trust in data collectors such as Google or Facebook is a stable, sticky individual characteristic that does not easily change even when individuals become aware of such a far-reaching policy change. Third, we know from research on contextual integrity and on context-specific privacy norms that there is an interplay of context characteristics that form what is perceived to be an appropriate data practice for a given scenario. It is unclear to which extent a general law like the GDPR is associated with the norms in such concrete situations in which particular privacy norms are at stake. Hence, one might need to measure behavior and attitudes in more concrete situations that are governed by such concrete contextual norms (Martin & Nissenbaum, 2017; Martin & Shilton, 2016a, 2016b; Nissenbaum, 2004, 2018).

A related explanation for our non-finding lies in the survey response process. When presented with a survey scale, respondents usually answer based on what currently resides in their mind (Zaller, 1992). Depending on the concepts presented in the question, respondents may have a wide variety of associations popping up when choosing their response (Bauer et al., 2017). Thinking of the response process, GDPR awareness as measured in our survey (in our case we introduced the GDPR question purposefully after the trust items) should have an impact on trust if an association with the GDPR appears in the minds of respondents when answering the trust elements. In other words, awareness can only become functional and have a positive effect when

respondents really think of the GDPR in their trust evaluation. Although this might be an explanation for the non-finding in our design, it does not necessarily invalidate our findings in terms of real-life relevance. While individuals are aware of the GDPR, this may not necessarily cross their mind, for instance, when they decide to share data when using a new smartphone app. This notion is supported by empirical evidence that the mere pointing to a privacy-related topic – no matter whether positive or problematic data practices are highlighted – increase respondents' carefulness in subsequent data disclosure, but *not* their stated privacy concerns (Marreiros et al., 2017).

Also, it is possible that policies such as the GDPR have long-term effects that we do not capture here. In principle, scholars assume that experiences affect trust (Bauer, 2015). If the GDPR leads to a decrease in data privacy violations, this could improve individuals' experiences over the course of a couple of years. Whether the GDPR really improves the situation remains to be seen. The corresponding design would need to compare populations that are subject to such a policy and populations that are not.

Finally, the GDPR might have had indirect effects on individuals' trust which is not reflected as such in our study. Although some people might not have been fully aware of the GDPR and its contents, many have been affected by its practical implications, increasing saliency. Individuals might have encountered more extensive and prominent cookie setting options on websites, particularly when these cookie settings are a requirement to enter a website. Another graspable instance is the updating of privacy policies of various online services, leading to many generic emails sent to their users. Also, in the non-digital realm, individuals were newly asked to give consent to the storage of their data, for example, by physicians. Such daily encounters might have rendered people more skeptical, cynic, and suspicious of various data practices (cf. Hermstrüwer and Dickert 2017; Lutz et al., 2020). In principle, we could imagine a situation where the same policy has diverse, contradicting effects on peoples' trust.

Our study is characterized by further limitations that provide venues for future research. The sample we rely on is a limitation of our study. While we are comfortable with giving our non-findings a causal interpretation, we cannot assume that we would find those same effects in the wider population. Including measures such as ours in representative samples would allow scholars to learn about population-level effects. This is relevant insofar as a more representative sample may also include populations that we do not cover here, for example, people with less intense Internet usage. In addition, our study is based on German data solely, hence, while our results may have some validity for the German case, studies conducted in other countries may yield different results. From a comparative perspective Germans seem to be more concerned about their privacy than many other Europeans (European Commission, 2015). Relatedly, it would be insightful to extend the set of data collectors for which we study trust. We picked Google and Facebook as they represented the most widely used platforms for search/email (Google) and social media (Facebook) at the time of our survey. However, the platform landscape is changing, and different platforms seem to embrace different privacy strategies. Hence, future studies would benefit from a comparison across a broader set of platforms such as Youtube, Amazon, Apple, Twitter and others.

Also, the measures we used carry a certain vagueness. For instance, the behavior referred to in the trust items is 'sharing data with third parties.' Both 'data' is vague in that it could refer to more or less sensitive data, and 'third parties' may also be of various



kinds, for example, advertisers in the case of Google or Facebook. Implicitly, throughout our paper (as is usually done) we assume that these questions and the concepts contained are interpreted similarly by respondents. While this point reflects the fundamental conflict between specificity and generality, research would benefit from even more precise survey questions. Fortunately, researchers have already started diving deeper into such complexity relying on vignette experiments (e.g., Horne & Przepiorka, 2019). Another strategy could be to probe respondents to explore how much interpretative variation is behind concepts such as ‘data’ or ‘third party.’

Finally, we studied the GDPR’s impact on trust. In our view, trust in itself is an informative indicator because it reflects people’s general expectations towards these platforms. However, to what extent trust interacts with concrete data sharing behavior – a link that is often taken for granted – requires further scrutiny (e.g., Bauer et al., 2019). As it stands, our study does not allow for predictions on whether and how different trust levels affect the usage of and extensiveness of data sharing with these platforms. However, various insightful theoretical accounts (e.g., Altman & Taylor, 1973; Petronio, 2002) may build the basis for further original empirical studies that explore this link.

Considering these and other limitations, we need to drive forward an increasingly urgent research agenda that explores the interaction between individuals’ preferences and behavior, privacy invading technologies, and policies that aim to regulate the latter. Such a research agenda may inform policy-makers that have taken up the challenge of reigning in technological advances to curb their negative consequences (cf. Lyon, 2001; Zuboff, 2019), which entails threats to the valuable right to privacy by surveillance (Büchi et al., 2020; Citron & Gray, 2013; Cohen, 2012), while allowing these technologies to unfold their positive potential. Trust in data collectors and data collection procedures, and therefore individuals’ comfort when they share data, is not necessarily fueled by the mere implementation of policies, as our findings suggest. How companies and national and local public institutions, such as data protection offices, handle data protection complaints and surveillance of data collectors may shape trust as well. The mechanism of how policy, private actors, and public institutions interplay to produce trust in data collectors remains an open question relevant to both the privacy research community and policy-makers and companies.

## Note

1. While the term data-sharing implies an action on part of the person sharing the data, we use the term to also designate the passive and unconscious sharing of data.
2. The GDPR was adopted by the Council of the European Union on 8 April 2016 and on 14 April 2016 by the European Parliament. Subsequently, the regulation entered into force on 24 May 2018 and its provisions became directly applicable in all member states on 25 May 2018. As the GDPR is a regulation, not a directive, it is directly binding and applicable in all member states (European Commission, 2019b).
3. A non-peer-reviewed study by Sobolewski and Paliński (2017) surveys students from Warsaw University ( $N = 143$ ) and presents them with a choice tasks to explore which aspects of the GDPR policy (e.g., the right to be forgotten or the right to migrate personal data) are perceived as more valuable. A non-peer-reviewed report by Aldighieri (2018) based on survey data ( $N = 1001$ ) explores consumers’ attitudes towards and perception of the GDPR from a consumer perspective.

4. We also add to a more general literature on ‘policy feedback.’ A vast literature has investigated feedback effects at the level of states and political elites (Campbell, 2012, p. 334). Research on policy feedback effects on mass publics centers on social welfare policy following the idea that it is one of the policy areas most salient to ordinary individuals (Campbell, 2012, p. 336). At first glance, privacy and data rights represent a less salient policy area. However, 2018 has seen several high-level scandals, e.g., the Cambridge Analytica Scandal that erupted in March 2018 that may have increased the salience of such topics. As far as we know, our study is the first to investigate policy effects in this policy subfield, and we situate it within broader research in this area.
5. Importantly, trust is here understood as a simple expectation that B behaves according to A’s preference. Some accounts define trust as believing in the benevolence of a trustee. However, the understanding here simply pertains to expectations regarding B’s behavior. Certainly, aside from third parties with sanctioning power, knowing that B has been trustworthy in the past or has other attributes may also affect A’s trust. And even if I don’t trust some organization, I might still decide to share data with it, for instance, because I have no other option, e.g., if this organization has a monopoly and I need its services.
6. There are various websites that provide GDPR enforcement data, e.g., <https://www.enforcementtracker.com/>.
7. For an explanation of the data underlying Google Trends, see Rogers (2016).
8. The sample was recruited using quotas for age, gender, and smartphone ownership. Only respondents who reported living in Germany were included in the sample. See Table A1 for statistics on how many respondents were discarded for various reasons.
9. In Wave 1 we used two different versions of the trust question, the standard trust scale depicted above and a subjective probability scale: *On a scale of 0% = ‘event will certainly not happen’ to 100% = ‘event will certainly happen’, how likely do you think it is that B uses your personal for internal purpose only, that is, not share the data with third parties?.* Respondents were randomly assigned to the two different scales and previous research indicates that it does not matter whether respondents answer on the normal scale or the probability scale (Bauer et al., 2019).
10. The data was coded by one coder (#1). We tested inter-coder reliability for a random subset of 200 responses which were coded by a second rater #2. The Cohen’s kappa for the two ratings lies at 0.89 (rater #2 coded 191 out of 200 responses in the same way as rater #1). Out of 6258 responses to the GDPR knowledge question across the three waves, 3793 responses were ‘Yes’, out of which 3683 provide some form of open-ended response to the probing question (only 110 didn’t). Answers ranged from very short ones (single words) to very long ones (the answer with the most words has 216; Median: 6 words, Mean: 8.6 words). Across all waves, out of the 3793 respondents who answered ‘Yes’ to the closed question on GDPR knowledge, our coding of open-ended responses declares 1250 respondents to not have provided an answer showing substantive understanding of the GDPR’s content.
11. Analyses were conducted in R. Tables were generated using the Stargazer R package (Hlavac 2014).
12. Device ownership has been shown to be strongly related to measures of digital literacy (Hargittai et al., 2019).
13. We also explored whether the effect of GDPR awareness is heterogeneous, i.e., is stronger among subsets of our sample that are high or low in digital literacy (operationalized through the number of devices they possess: high = number of devices  $\geq 4$  ( $N = 247$ ) and low = number of devices  $\leq 2$  ( $N = 459$ )). This was not the case.
14. Overall, it appears that awareness levels in our study are similar to those in other studies. On 1 March 2018 YouGov reports that around three quarters (72%) of British adults haven’t heard of GDPR (Glanville 2018).
15. We also explored whether the effect of GDPR awareness is heterogeneous, i.e., is stronger among subsets of our sample that are high or low in digital literacy (operationalized through the number of devices they possess: high = number of devices  $\geq 4$  ( $N = 247$ ) and low =

number of devices  $\leq 2$  ( $N = 459$ )). This was not the case. In addition, we further explore the relationship between generalized trust, privacy concern, and our trust judgments. Figure A5 depicts a correlation matrix and correlations reach a maximum of 0.4, relevant but not particularly high in our view. In additional analyses, we re-estimated our difference-in-differences models using generalized trust and privacy concern as outcome variables (see reproduction files). We do not find effects reflecting the findings for our trust judgments.

## Disclosure statement

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

## Funding

This work was supported by the German Research Foundation (DFG) through the Collaborative Research Center SFB2 884 ‘Political Economy of Reforms’ (Project A9) [139943784 to Markus Frölich, F.K., and F.K.]. Part of Frederic Gerdon’s time was funded by Volkswagen Foundation (grant ‘Consequences of Artificial Intelligence for Urban Societies’). Part of Frauke Kreuter’s time in 2018 was supported by a Facebook contract with Pro Unlimited.

## Notes on contributors

**Paul C. Bauer** is a research fellow at the Mannheim Centre for European Social Research and pursues research in political behavior, political communication, and computational social science. His current research interests comprise the believability of misinformation and the social media activity and influence of politicians. His work has appeared in *Political Communication*, *Public Opinion Quarterly*, *Political Behavior*, *PLOS One*, and the *European Sociological Review*. E-mail: paul.bauer@mzes.uni-mannheim.de.

**Frederic Gerdon** is a doctoral researcher at the Mannheim Centre for European Research at the University of Mannheim, Germany, and at the Department of Statistics of the Ludwigs Maximilians University Munich, Germany. He currently researches social consequences of digitization and algorithmic decision-making, with a particular focus on social inequality and privacy, and mainly employs quantitative methods such as survey experiments. E-mail: fgerdon@mail.uni-mannheim.de.

**Florian Keusch** is a Professor (interim) of Statistics and Methodology at the University of Mannheim, Germany, and Adjunct Assistant Professor at the Joint Program in Survey Methodology (JPSM), University of Maryland, U.S. His current research interests comprise nonresponse and measurement error in (mobile) Web surveys and passive mobile data collection and attitudes towards data sharing. His work has been published in *Sociological Methods & Research*, *Public Opinion Quarterly*, and *Social Science Computer Review*. E-mail: f.keusch@uni-mannheim.de.

**Frauke Kreuter** is Professor of Statistics and Data Science for the Social Sciences and Humanities at the Ludwig-Maximilians-University of Munich (Germany) and co-director of Data Science Centers at the University of Maryland (USA) and Mannheim (Germany). Current research interests comprise data quality, privacy, and the combination of multiple data sources for statistics production. Her work has been published in the *Annual Reviews of Statistics and its Application*, *Harvard Data Science Review*, and *Public Opinion Quarterly*. E-mail: frauke.kreuter@stat.uni-muenchen.de.

**David Vannette** is a Visiting Scholar in Political Science at the University of California, Davis. His current research interests include question and questionnaire design, survey nonresponse, and measurement error in a global context, primarily in mobile web surveys. He also has an interest in political psychology and has recently published on the psychological experiences of Latina/o immigrants to the U.S. His work has been published in the *American Journal of Political Science*,

Journal of the Royal Statistical Society, Policy Studies Journal, Research Quality Forum, several book chapters, and recently edited the Palgrave Handbook of Survey Research. E-mail: dave.vannette@gmail.com.

## ORCID

Paul C. Bauer  <http://orcid.org/0000-0002-8382-9724>

Frederic Gerdon  <http://orcid.org/0000-0003-4442-6698>

Florian Keusch  <http://orcid.org/0000-0003-1002-4092>

Frauke Kreuter  <http://orcid.org/0000-0002-7339-2645>

## References

- Altman, I., & Taylor, D. A. (1973). *Social penetration: The development of interpersonal relationships*. Holt, Rinehart & Winston.
- EU General Data Protection Regulation (GDPR), no. REGULATION (EU) 2016/679, EUROPEAN PARLIAMENT, COUNCIL (2016).
- Aldighieri, R. (2018). *GDPR: A consumer perspective 2018*. acxiom. [https://dma.org.uk/uploads/misc/5af5497c03984-gdpr-consumer-perspective-2018-v1\\_5af5497c038ea.pdf](https://dma.org.uk/uploads/misc/5af5497c03984-gdpr-consumer-perspective-2018-v1_5af5497c038ea.pdf)
- Allen, D. W. E., Berg, A., Berg, C., Markey-Towler, B., & Potts, J. (2018). *Some economic consequences of the GDPR*. <https://doi.org/10.2139/ssrn.3160404>
- Angrist, J. D., & Pischke, J.-S. (2008). *Mostly harmless econometrics: An empiricist's companion*. Princeton University Press.
- Anthony, D., Campos-Castillo, C., & Horne, C. (2017). Toward a sociology of privacy. *Annual Review of Sociology*, 43(1), 249–269. <https://doi.org/10.1146/annurev-soc-060116-053643>
- Baier, A. (1986). Trust and antitrust. *Ethics*, 96(2), 231–260. <https://doi.org/10.1086/292745>
- Baker, L. (2017). The impact of the General Data Protection Regulation on the banking sector: Data subjects' rights, conflicts of laws and Brexit. *Journal of Data Protection & Privacy*, 1(2), 137–145.
- Barnard-Wills, D., Pauner Chulvi, C., & De Hert, P. (2016). Data protection authority perspectives on the impact of data protection reform on cooperation in the EU. *Computer Law & Security Review*, 32(4), 587–598. <https://doi.org/10.1016/j.clsr.2016.05.006>
- Bashir, M., Hayes, C., Lambert, A. D., & Kesan, J. P. (2015). Online privacy and informed consent: The dilemma of information asymmetry. *Proceedings of the Association for Information Science and Technology*, 52(1), 1–10. <https://doi.org/10.1002/pr2.2015.145052010043>
- Bauer, P. C. (2015). Negative experiences and trust: A causal analysis of the effects of victimization on generalized trust. *European Sociological Review*, 31(4), 397–417. <https://doi.org/10.1093/esr/jcu096>
- Bauer, P. C. (forthcoming). Conceptualizing trust and trustworthiness. In R. Barradas De Freitas & S. Lo Iacono (Eds.), *Trust matters: Cross-disciplinary essays* (pp. 1–16). Hardt Publishing.
- Bauer, P. C., Barberá, P., Ackermann, K., & Venetz, A. (2017). Is the left-right scale a valid measure of ideology? *Political Behavior*, 39(3), 553–583. <https://doi.org/10.1007/s11109-016-9368-2>
- Bauer, P. C., & Freitag, M. (2018). Measuring trust. In E. M. Uslaner (Ed.), *The Oxford handbook of social and political trust* (pp. 1–27). Oxford University Press.
- Bauer, P. C., Keusch, F., & Kreuter, F. (2019). Trust and cooperative behavior: Evidence from the realm of data-sharing. *PLoS ONE*, 14(8), 1–18. <https://doi.org/10.1371/journal.pone.0220115>
- Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., & Rost, M. (2016). A process for data protection impact assessment under the European general data protection regulation. *Privacy Technologies and Policy*, 9857, 21–37. [https://doi.org/10.1007/978-3-319-44760-5\\_2](https://doi.org/10.1007/978-3-319-44760-5_2)
- Binns, R. (2017). Data protection impact assessments: A meta-regulatory approach. *International Data Privacy Law*, 7(1), 22–35. <https://doi.org/10.1093/idpl/ipw027>
- Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, 82(5), 977–1008. <https://doi.org/10.1177/0003122417725865>

- Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2020). The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law & Security Review*, 36, 105367. <https://doi.org/10.1016/j.clsr.2019.105367>
- Burt, R. S., & Knez, M. (1995). Kinds of third-party effects on trust. *Rationality And Society*, 7(3), 255–292. <https://doi.org/10.1177/1043463195007003003>
- Buskens, V., Raub, W., & van der Veer, J. (2010). Trust in triads: An experimental study. *Social Networks*, 32(4), 301–312. <https://doi.org/10.1016/j.socnet.2010.05.001>
- Campbell, A. L. (2012). Policy makes mass politics. *Annual Review of Political Science*, 15(1), 333–351. <https://doi.org/10.1146/annurev-polisci-012610-135202>
- Campos-Castillo, C., & Anthony, D. (2019). Situated trust in a physician: Patient health characteristics and trust in physician confidentiality. *The Sociological Quarterly*, 60(4), 559–582. <https://doi.org/10.1080/00380253.2018.1547174>
- Ciriani, S. (2015). *The economic impact of the European reform of data protection*. <https://papers.ssrn.com/abstract=2674010>
- Citron, D. K., & Gray, D. (2013). Addressing the harm of total surveillance: A reply to professor Neil Richards. *Harvard Law Review*, 126(7), 262–274.
- Cohen, J. E. (2012). What privacy is for. *Harvard Law Review*, 126(7), 1904–1933. <https://heinonline.org/HOL/P?h=hein.journals/hlr126&i=1934>
- Croissant, Y., & Millo, G. (2008). Panel data econometrics in R: The plm package. *Journal of Statistical Software*, 27(2), 1–43. <https://doi.org/10.18637/jss.v027.i02>
- de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the crowd: The privacy bounds of human mobility. *Scientific Reports*, 3(1), 1376. <https://doi.org/10.1038/srep01376>
- The Economist. (2018). America should borrow from Europe’s data-privacy law. *The Economist*. <https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law>
- European Commission. (2015). Special eurobarometer 431 “data protection”/ Wave EB83.1. <https://www.dx.doi.org/10.2838/552336>
- European Commission. (2019a). *Data protection rules as a trust-enabler in the EU and beyond – taking stock. Communication from the Commission to the European Parliament and the Council*. [https://ec.europa.eu/info/sites/info/files/aid\\_development\\_cooperation\\_fundamental\\_rights/aid\\_and\\_development\\_by\\_topic/documents/communication\\_2019374\\_final.pdf](https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/communication_2019374_final.pdf)
- European Commission. (2019b, October 18). *EU data protection rules*. [https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules\\_en](https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en)
- Faitelson, Y. (2017, December 4). Yes, the GDPR will affect your U.S.-based business. *Forbes Magazine*. <https://www.forbes.com/sites/forbestechcouncil/2017/12/04/yes-the-gdpr-will-affect-your-u-s-based-business/>
- Feiner, L. (2019, April 24). *Facebook says the FTC privacy inquiry could cost as much as \$5 billion*. CNBC. <https://www.cnbc.com/2019/04/24/facebook-estimates-up-to-5-billion-loss-in-ftc-privacy-inquiry.html>
- Freudiger, J., Shokri, R., & Hubaux, J.-P. (2012). Evaluating the privacy risk of location-based services. *Financial Cryptography and Data Security*, 7035, 31–46. [https://doi.org/10.1007/978-3-642-27576-0\\_3](https://doi.org/10.1007/978-3-642-27576-0_3)
- Glanville, B. (2018, March 1). 72% of Brits haven’t heard about GDPR. *YouGov*. <https://yougov.co.uk/topics/politics/articles-reports/2018/03/01/72-brits-havent-heard-about-gdpr>
- Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703–705. <https://doi.org/10.2501/IJMR-2017-050>
- Golder, S. A., & Macy, M. W. (2014). Digital footprints: Opportunities and challenges for online social research. *Annual Review of Sociology*, 40(1), 129–152. <https://doi.org/10.1146/annurev-soc-071913-043145>
- Greengard, S. (2018). *ACM: Digital library: Communications of the ACM*. dl.acm.org. <https://dl.acm.org/doi/fullHtml/10.1145/3276744>



- Hacker, P., & Petkova, B. (2017). Reining in the big promise of big data: Transparency, inequality, and new regulatory frontiers. *Northwestern Journal of Technology and Intellectual Property*, 15, i.
- Hermstrüwer, Y., & Dickert, S. (2017). Sharing is daring: An experiment on consent, chilling effects and a salient privacy nudge. *International Review of Law and Economics*, 51, 38–49. <https://doi.org/10.1016/j.irl.2017.06.001>
- Hargittai, E., Piper, A. M., & Morris, M. R. (2019). From internet access to internet skills: Digital inequality among older adults. *Universal Access in the Information Society*, 18(4), 881–890. <https://doi.org/10.1007/s10209-018-0617-5>
- Horne, C., & Przepiorka, W. (2019). Technology use and norm change in online privacy: Experimental evidence from vignette studies. *Information, Communication and Society*, 1–17. <https://doi.org/10.1080/1369118X.2019.1684542>
- Kang, C. (2019, July 12). F.T.C. approves Facebook fine of about \$5 billion. *The New York Times*. <https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html>
- Keusch, F. (2019). *Trust, privacy & data sharing, ZA6979 Data file Version 1.0.0* [Data set]. <https://doi.org/10.4232/1.13248>
- Kohler, U. (2019). Possible uses of nonprobability sampling for the social sciences. *Survey Methods: Insights from the Field*, 1–12. <https://doi.org/10.13094/SMIF-2019-00014>
- Lindsey, N. (2019, November 25). Google will restrict sharing of user data for Google ads under EU privacy pressure. *CPO Magazine*. <https://www.cpomagazine.com/data-privacy/google-will-restrict-sharing-of-user-data-for-google-ads-under-eu-privacy-pressure/>
- Liu, V., Musen, M. A., & Chou, T. (2015). Data breaches of protected health information in the United States. *JAMA: The Journal of the American Medical Association*, 313(14), 1471–1473. <https://doi.org/10.1001/jama.2015.2252>
- Lutz, C., Hoffmann, C. P., & Ranzini, G. (2020). Data capitalism and the user: An exploration of privacy cynicism in Germany. *New Media & Society*, 22(7), 1168–1187. <https://doi.org/10.1177/1461444820912544>
- Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. McGraw-Hill Education.
- Marreiros, H., Tonin, M., Vlassopoulos, M., & Schraefel, M. C. (2017). “Now that you mention it”: A survey experiment on information, inattention and online privacy. *Journal of Economic Behavior & Organization*, 140, 1–17. <https://doi.org/10.1016/j.jebo.2017.03.024>
- Martin, K., & Nissenbaum, H. (2017). Measuring privacy: an empirical test using context to expose confounding variables. *Science and Technology Law Review*, 18(1). <https://doi.org/10.7916/stlr.v18i1.4015>
- Martin, K., & Shilton, K. (2016a). Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology*, 67(8), 1871–1882. <https://doi.org/10.1002/asi.23500>
- Martin, K., & Shilton, K. (2016b). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society*, 32(3), 200–216. <https://doi.org/10.1080/01972243.2016.1153012>
- Mayer-Schönberger, V., & Cukier, K. (2012). *Big data: A revolution that transforms how we work, live, and think*. Houghton Mifflin Harcourt.
- McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *ISJLP*, 4(3), 543–568.
- Michaelidou, N., & Micevski, M. (2019). Consumers’ ethical perceptions of social media analytics practices: Risks, benefits and potential outcomes. *Journal of Business Research*, 104, 576–586. <https://doi.org/10.1016/j.jbusres.2018.12.008>
- Morrissey, S. (2016). Take notice! The legal and commercial impact of the General Data Protection Regulation’s rules on privacy notices. *Journal of Data Protection & Privacy*, 1(1), 46–52.
- Nippert-Eng, C. E. (2010). *Islands of privacy*. University of Chicago Press.
- Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79, 119.
- Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.



- Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics*, 24(3), 831–852. <https://doi.org/10.1007/s11948-015-9674-9>
- O'Brien, C. (2018, December 13). Google Ireland takes the reins for European services. *The Irish Times*. <https://www.irishtimes.com/business/technology/google-ireland-takes-the-reins-for-european-services-1.3730721>
- Peretti, K. K. (2008). Data breaches: What the underground world of carding reveals. *Santa Clara Computer & High Technology Law Journal*, 25, 375.
- Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. SUNY Press.
- Presthus, W., & Sørsum, H. (2018). Are consumers concerned about privacy? An online survey emphasizing the General Data Protection Regulation. *Procedia Computer Science*, 138, 603–611. <https://doi.org/10.1016/j.procs.2018.10.081>
- Richardson, L. (1988). Secrecy and status: The social construction of forbidden relationships. *American Sociological Review*, 53(2), 209–219. <https://doi.org/10.2307/2095688>
- Rogers, S. (2016, July 1). *What is Google Trends data — And what does it mean?* Medium; Google News Lab. <https://medium.com/google-news-lab/what-is-google-trends-data-and-what-does-it-mean-b48f07342ee8>
- Rubinstein, I., & Petkova, B. (2018). *The international impact of the general data protection regulation*. <https://papers.ssrn.com/abstract=3167389>
- Seligman, A. B. (2000). *The problem of trust*. Princeton University Press.
- Sobolewski, M., & Paliński, M. (2017). *How much consumers value on-line privacy? Welfare assessment of new data protection regulation (GDPR)* (No. 2017-17). Faculty of Economic Sciences, University of Warsaw. <https://ideas.repec.org/p/war/wpaper/2017-17.html>
- Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, 2016(6), 5–8. [https://doi.org/10.1016/S1353-4858\(16\)30056-3](https://doi.org/10.1016/S1353-4858(16)30056-3)
- Thompson, S. A., & Warzel, C. (2019, December 19). Twelve million phones, one dataset, zero privacy. *The New York Times*. <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>
- van Ooijen, I., & Vrabec, H. U. (2018). Does the GDPR enhance consumers' control over personal data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, 1–17. <https://doi.org/10.1007/s10603-018-9399-7>
- Wang, R. Y., & Ng, C. N. (2015). Can centralized sanctioning promote trust in social dilemmas? A two-level trust game with incomplete information. *PLoS ONE*, 10(4), e0124513. <https://doi.org/10.1371/journal.pone.0124513>
- Watts, D. J. (2004). The “new” science of networks. *Annual Review of Sociology*, 30(1), 243–270. <https://doi.org/10.1146/annurev.soc.30.020404.104342>
- Zaller, J. (1992). *The nature and origins of mass opinion*. Cambridge University Press.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.