Journal of European Public Policy

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rjpp20

Citizens’ agreement to share personal data for public policies: trust and issue importance

Philipp Trein & Frédéric Varone

To cite this article: Philipp Trein & Frédéric Varone (2024) Citizens’ agreement to share personal data for public policies: trust and issue importance, Journal of European Public Policy, 31:9, 2483-2508, DOI: 10.1080/13501763.2023.2205434

To link to this article: https://doi.org/10.1080/13501763.2023.2205434

JOURNAL OF EUROPEAN PUBLIC POLICY
2024, VOL. 31, NO. 9, 2483–2508
https://doi.org/10.1080/13501763.2023.2205434

Routledge
Taylor & Francis Group

OPEN ACCESS

Citizens’ agreement to share personal data for public policies: trust and issue importance

Philipp Trein [a] and Frédéric Varone [b]

[a]Institute of Political Studies, University of Lausanne, Lausanne, Switzerland; [b]Department of Political Science and International Relations, University of Geneva, Geneva, Switzerland

ABSTRACT
The digitalisation of public policy requires that the State uses citizens’ personal data. Although researchers agree that data privacy is important, we know little about the conditions under which citizens approve of their personal data being used in different policy domains. This study relies on data from original surveys conducted in Switzerland to demonstrate that citizens’ willingness to share their data with the State is low and varies across policy domains. Support for sharing is significantly higher when the data are used to prevent benefit fraud in social assistance or to improve health research than when they are used to fight tax evasion or to prevent crime and terrorism. Nevertheless, we also argue that the more citizens trust government and the more important they consider a policy issue to be, the more likely they are to share their data with the State officials in charge of the relevant policy. Previous use of apps also increases citizens’ agreement for the policy-related use of their personal data.

ARTICLE HISTORY Received 14 July 2022; Accepted 18 April 2023

KEYWORDS Privacy; policy-making; health; taxes; welfare; security

Introduction

The usage of information and communication technologies (ICTs) comes along with the collection of citizens’ data and increases the likelihood of surveillance and manipulation by private companies (Lupton, 2016; Lyon, 2002). Beyond the private sphere, governments use ICTs to collect personal data for policy-making processes and the delivery of public services. For example, health data collected in public data repositories can be used to improve genetic research and health services (Jensen *et al*., 2012), whereas telephone

CONTACT Philipp Trein josefphilipp.trein@unil.ch Institute of Political Studies, University of Lausanne, Géopolis 4126, 1015 Lausanne, Suisse

Supplemental data for this article can be accessed online at https://doi.org/10.1080/13501763.2023.2205434

data, criminal records, and other information are important to implement predictive policing (Ferguson, 2017; Shapiro, 2017). It seems obvious that using digital data can improve public policies, however, such practices come also along with new possibilities for intruding citizens' privacy. This article focuses on studying under which conditions citizens are likely to consent to such an intrusion into their privacy.

Privacy scholars from different disciplines have analysed the challenge of protecting personal data from potential privacy infringements by companies (e.g., Acquisti *et al*., 2013; Bach & Newman, 2007; Benndorf & Normann, 2018; Caudill & Murphy, 2000; Evens & Van Damme, 2016; Happ *et al*., 2016; Martin & Nissenbaum, 2016; Urbonavicius *et al*., 2021) and political parties (e.g., Dobber *et al*., 2019). The literature has pointed out that the automatic collection of personal data creates a risk for other uses of this data later, and, that individuals tend to underestimate the risk of such data collection by companies (Lupton, 2016; Zimmer *et al*., 2020). Scholars have analysed the usage of ICTs and algorithms for the provision of public services (e.g., Ahn & Bretschneider, 2011; Björklund, 2016; Chadwick & May, 2003; Ciusi *et al*., 2020; Dunleavy *et al*., 2006; Fang, 2002; Lee *et al*., 2011; Silcock, 2001; Twizeyimana & Andersson, 2019), however, this research focuses rarely on the conditions under which individuals are comfortable to share their date with the State for public policies. This is surprising because scholars have also noticed a privacy paradox regarding the usage of personal data for public policy. For example, once Congressional lawmakers faced criticisms about potential government surveillance, they continued to work with private companies behind closed doors to ensure government surveillance capacities (Rider, 2018). Such a depoliticisation of State investigation capabilities might however undermine the democratic legitimacy of these policies even further. Thus, we need to know more about the extent to which citizens are willing to share their personal data for public policy to determine under which conditions such actions are politically feasible and legitimate. This a major topic for the democratic governance of ICTs.

This article contributes to the literature by analysing when (and potentially why) individuals are willing to share their data with public authorities for specific public policies. Therefore, we embark into a comparative empirical analysis of three representative surveys that were conducted in Switzerland in March 2020, November 2020, and March 2021. Our evidence shows a clear difference between policies: respondents are more likely to share their health and social security data than their banking and telephone data.

Beyond these differences between policy fields, we seek to better understand the elements that are associated with individuals' willingness to share data for public policy. Therefore, we assume that providing their individual data for public policy entails a dilemma for individuals. On the one hand, they might want to share their data if they are used for policies that address problems that are important to them; but on the other hand, they are afraid of the potential infringement into their privacy that comes along with this. Thus, trust (Rousseau *et al*., 1998) is likely to play an important role for the extent to which individuals are ready to share their data.

Our regression analyses at the individual level confirm the importance of this potential paradox. Citizens are more likely to share their data if they believe that the policy problem the State seeks to solve is important to them and if they trust their government. The association of issue importance and data sharing becomes stronger the more individuals trust the national government. Previous use of apps requiring sharing personal data also increases the willingness to provide such data for public policy. By contrast, differences in ideology seem to have no effect on whether individuals are willing to share their personal data for public policy or not. We conclude by putting these findings in a broader theoretical perspective and offer a roadmap for policymakers.

Background and research approach

Scholars agree that citizens want their data to be protected because they feel uncertain about their privacy being respected in the digital world (Acquisti *et al*., 2015; Bennett, 2011, 2016; de Goede, 2014; EU, 2015; Morse & Birnhack, 2020). Data from the 2015 Eurobarometer shows that 69 per cent of the respondents in the 28 members of the European Union are concerned that the authorities and the private companies holding personal information might use it for a purpose other than the one for which it was collected (EU, 2015).[1] Similarly, we know that the protection of personal data in several policy fields, such as genetics and policing, is a key citizen concern (Bearth & Siegrist, 2020; Macnish *et al*., 2020; Middleton *et al*., 2020). A recent survey from Austria shows that around 38 per cent of respondents consent to sharing their data to counteract the COVID-19 crisis, and 36 per cent consent to their data being used for public policies that maintain public safety (Kittel *et al*., 2021). In a similar vein, citizens in Germany, Spain, France, and the United Kingdom are ready to share their personal data for public policies aiming at reducing criminality by using new technologies, such as facial recognition (Ziller & Helbling, 2021).

Importantly, scholars have demonstrated that citizens are willing to share their data rather with public than with private entities and for a limited rather than an unlimited period (Belle *et al*., 2021). Horvath *et al*. (2022) showed that individuals are more willing to share their health-related data in a database that is largely maintained by a National Health Service than by central government. We also know that individuals who trust government services are more likely to share their data for public policy (Murphy *et al*., 2021). The next step for this research is to deepen our understanding about under which conditions individuals are willing to share their data for the purposes of conducting different types of public policies.

This article contributes to the literature on digitalisation and public policies broadly defined by assessing the willingness to share data for public policies. Our added value is to put the insights related to COVID apps (e.g., Horvath *et al*., 2022), the health sector (e.g., Belle *et al*., 2021), and crime reduction (e.g., Ziller and Helbling, 2021) into a broader perspective by including other policy domains. The aim of this study is twofold. Firstly, we want to understand if there are differences between the purposes for which citizens are willing to share their sensitive personal data with public policy-makers. Secondly, we want to understand if we can identify factors that might potentially be associated to the overall differences between citizens regarding their willingness to share data for public policies.

To study the conditions under which individuals are willing to share their personal data with the state, we focus on four specific and realistic issues where personal data has been used for public policy interventions. Table 1 shows the policy fields addressed as well as the survey items that we used to capture willingness to share personal data for public policy. More details can be found in the methods section and the supplementary materials.

Our selection combines four very different policy issues. We frame all the survey questions in a way that makes it not too difficult for citizens to agree because it is well known that privacy is important and they individuals are probably weary that their data might be abused by government (Acquisti, John, and Loewenstein, 2013; Bach and Newman, 2007; Caudill and Murphy, 2000). Nevertheless, it is unlikely that all citizens will consent in a similar way to sharing their personal data for all public policies. In the following, we formulate hypotheses related to a 'calculus-based trust' approach (see Rousseau *et al*. 1998: 399) that could potentially explain why individuals might differ in their willingness to share their sensitive data with public authorities across these four policy domains.

Why would individuals agree to share their personal data for public policy?

In their seminal article, Rousseau *et al*. (1998:395) defined trust as '*a psychological state comprising the intention to accept vulnerability based upon positive*

Table 1. Four specific issues for personal data use in public policy.

Policy field	Specific issue
Welfare	*I consent to sharing my social insurance data to create a more efficient social system with less fraud*
Health	*I consent to sharing my health data to support research for medical progress*
Taxation	*I consent to sharing data about my bank accounts to optimize the fight against tax fraud*
Security	*I consent to sharing my telephone data (connections and movement profile) to improve the prevention of crime and terrorism*

expectations of the intentions or behavior of another'. This approach is particularly relevant for the research question we address in this empirical study. Indeed, we focus on the relationship between the State and citizens, who may trust (or not) the government for using their personal data in policymaking processes and service delivery. Such a relationship encompasses two conditions for trust to emerge, as suggested by Rousseau *et al*. (1998).

On the one hand, vulnerability is the first condition creating an opportunity for trust. Accepting that the State uses personal and sensitive data is always risky because citizens are not sure that the State will act appropriately and protect fundamental civil rights. Citizens may loss something if the State does not limit privacy breach to the strict minimum. In line with the assumptions of the liberal vision of democracy, which dates back to John Locke and John Stuart Mill, the State could indeed represent the greatest danger to privacy (Bennet and Raab, 2006): Citizens' privacy and individual rights must be protected from State intrusion in order to avoid the emergence of an authoritarian State like the one illustrated by the social credit system implemented in China.

Authors embracing the Foucaultian approach go one step further and argue that the protection of individuals' privacy—the one that liberal theories advocate for—is not enough to prevent the development of a disciplinary surveillance system (e.g., Gandy, 1993).[2] Whatever theoretical and normative benchmark is deployed to assess the potential danger of the State using personal data, it seems reasonable to assume that citizens will only be prone to sharing their data with the State, if they accept to become vulnerable and trust democratic institutions and processes (e.g., Murphy *et al*., 2021). They should be convinced that public authorities will not instrumentalise their personal data to reduce their freedom and limit their constitutional rights. Our first hypothesis is based on this rationale and stipulates that the citizens reporting that they trust their government are more likely to share their data with the State in all policy domains. Note that this relationship between trust in government and the collaboration of citizens regarding public policies has been shown related to the COVID-19 pandemic: those who trust government are more likely to get vaccinated against the virus (Debus and Tosun, 2021; Wynen *et al*., 2022).

On the other hand, interdependence between the State and citizens' interests is the second condition for trust to be stabilised. Concretely, the policy objectives as defined by the State cannot be achieved without the reliance upon the citizens' willingness to share their personal data. Vice versa, citizens expect that the public policies decided and implemented by the State will be beneficial to them. Citizens who trust their government probably expect that public authorities will adopt transversal regulations, such as the European General Data Protection Regulation (GDPR), to protect their private sphere and individual rights (see Bocquet, 2023). In doing so, the government—

namely, its data protection agency—works as a classical regulator who develops, implements, and enforces data protection measures. At the same time, the government also is one of the targets of its own privacy policy. Indeed, various ministries and administrative services collect, store, and use personal data. As Weber initially suggested and authors such as Beniger (1986), Desrosières (1993), and Mau (2017) later highlighted, public bureaucracies have a strong motivation and a natural tendency to monitor citizens' sensitive data: Administrative services need to rationalise public service delivery to be able to grant social rights (e.g., welfare policies), enforce obligations (e.g., taxation policy), plan investment in public infrastructure (e.g., transport policy), or to sanction deviant behaviour (e.g., criminal policy). A recently published study suggests that context strongly matters for the usage of algorithms in the public sector (Wenzelburger *et al*., 2023). Accordingly, it makes sense to investigate whether citizens' willingness to share their data with the State depends on the policy problems that public bureaucracies aim to solve through a data-based policy approach.

We assume that citizens will accept a stronger reduction of their privacy if their data are used to address a policy problem that they personally consider to be very important. In other words, citizens are likely to consent to their personal data being used for a highly important policy issue, but they will be strongly reluctant to allow the State to process their personal data to address a policy problem of low priority. Previous studies have identified 'issue importance' as a strong predictor of political behaviour such as voting: Citizens elect candidates from the party that addresses the policy issues they consider most important to their personal lives (Bélanger and Meguid, 2008; Budge and Farlie, 1983). By analogy, we assume that citizens will accept to share their data with the State only if public bureaucracies focus on a policy problem that citizens deem important. The second hypothesis states that citizens who believe that a policy issue is important are more likely to share their data with the State in that policy domain.

Furthermore, the 'calculus-base trust' approach suggests to combine both conditions and, thus, to look at the interaction between the general trust in government and the personal importance given to a policy issue. If citizens generally trust the government and, in addition, perceive the policy problem at stake as highly important, then they are more likely to accept to take a bigger risk—by sharing their personal data with the State—to achieve a policy objective generating a personal and collective benefit. High trust results in the decision to cooperate with the State, which lead to policy gains. However, this relationship is always contingent: the trustor (i.e., citizen) should believe in the positive intentions of the trustee (i.e., the State) and is ready to take high risk (i.e., sharing sensitive data) only if the expected gains (i.e., solving an important policy problem) are high. This third hypothesis also contributes to explain why we observe variation across policy domains.

The fourth hypothesis also assumes that differences across policy domains matter. Moreover, it supposes that political ideology and, specifically, the policy positions citizens adopt are crucial to explain their behaviour (intent). Indeed, the 'issue ownership' approach has demonstrated that citizens vote for those political parties they consider most apt to handle important policy issues (Bellucci, 2006; Green and Jennings, 2012; Lachat, 2014; Petrocik, 1996; Walgrave *et al*., 2015). Citizens vote for the party that appears to the one most able to implement the policy solutions they prefer. If we apply this general idea to our research object, we can postulate that citizens will only consent to share their personal data with the State if the policy objectives pursued in that policy domain match their own policy preferences and political ideology. This implies that citizens with different ideologies (captured by their party affiliations) will display different levels of willingness to share their personal data depending on the congruence between their positions and the officially stated policy objectives.

This generic formulation of the fourth hypothesis can be translated into more specific expectations that cover the four policy domains compared in this study. Based on the positions that the Swiss political parties embrace on the policy issues they own (see Lanz and Sciarini, 2016), our hypothesis implies that citizens leaning to the right are more likely to consent to the State using their data in the Welfare and Security policy domains but not regarding Health and Banking policy. In contrast, citizens leaning to the left are more likely to agree that the State use their data in the domains of Health research and Banking policy. Indeed, the electoral manifestoes and political agendas of (radical) right parties strongly focus on the fight against 'social benefits abusers' and (foreign) criminals and terrorists. Whereas left-parties have generally taken up capacity-building in public health research and regulatory measures to deter tax frauds and promote fiscal justice (e.g., Varone *et al*., 2014).

Finally, we should not only focus on citizens and State actors to explain individuals' readiness to share their personal data. Of course, citizens especially trust their national governments (66 per cent of the respondents to the Eurobarometer 2015 in the 28 members of the EU) and healthcare and medical institutions (74 per cent of the same group of respondents) to protect their personal data, while they hold less trust in banks and financial institutions (56 per cent), shops and stores (40 per cent), and telecommunications companies (33 per cent) (EU 2015). This is not surprising, since public authorities are probably more constrained by public regulations than private businesses and should follow citizens' general interests (instead of private and commercial interests) when they use sensitive data.

Nevertheless, it is obvious that the number of electronic devices in our daily life is growing quickly. Consequently, the type and quantity of personal data that are collected, stored, and used (mostly by private businesses) are also exploding. The technical complexity and the globalised dimension of this digitalisation process also increase the lack of transparency in privacy issues. It thus becomes difficult, if not impossible, for citizens to accurately understand who collects and processes their personal data and for what purpose they do so (Lupton, 2016; Lyon, 2002). Nevertheless, not all individuals react to the potential threat on their privacy in the same way. Some citizens deliberately refuse to use search engines, websites, operating systems, Internet providers or apps that allow private firms or public authorities to collect sensitive personal data (see Hirsch, 2011). These attitudes and behaviours can be motivated by the 'slippery slope' or 'foot-in-the door' psychological argument (van der Burg, 1991): the opponents of data sharing assume that using a search engine or an app is a relatively small, but insidious, first step that will eventually lead to a chain of related decisions (i.e., using additional apps and sharing more and more data) culminating in some significant and negative result (i.e., a complete loss of privacy) (Lupton, 2016). In contrast, other citizens do not fear such a risk and readily use available apps without too much hesitation. It is plausible that these citizens will not be reluctant to allow that the State also use their data in order to improve policy-making and service delivery. Accordingly, our fifth hypothesis assumes that citizens who already share their personal data in apps are more likely to consent to the State using their data in all policy domains.

Table 2 summarises the hypotheses that emerge from this discussion.

Data and measurements

This study focuses on citizens' willingness to share their personal data for the purposes of improving public policy. We capture this willingness through three different surveys conducted in Switzerland. However, the main analysis

Table 2. Overview of independent variables and hypotheses.

Independent variables	Hypothesis formulations
H1: Trust in government	Citizens who report that they trust the government are more likely to share their data with the State in all policy domains.
H2: Issue importance	Citizens who report that the policy problem to be solved is important to them are more likely to share their data with the State in the particular policy domain.
H3 Interaction effect	Citizens who report that they trust the government and find that the policy problem to be solved is important to them are more likely to share their data with the State in the particular policy domain.
H4: Partisan ideology	Citizens are more likely to share their data with the State if their partisan affiliation/ideology is congruent with the policy objectives
H5: App use	Citizens who already share their personal data in apps are more likely to share their data with the State in all policy domains.

in this article is based on the second and the third of these surveys, which we discuss in the following. Information regarding the first sample can be found in the supplementary materials.

The *second* sample comes from an online survey that was fielded in November 2020 and collected data on 1,458 respondents. This sample is representative on age, gender, educational attainment, and region of residence according to the data published by the national statistical agency of Switzerland (Bundesamt für Statistik). The *third* sample of respondents is like the second survey in terms of its representativity and the way in which variables are measured. It was fielded between March and April 2021 and obtained $N = 2{,}102$ responses.

The surveys include the variables we use to measure respondents' agreement to share their personal data for the purposes of formulating public policy and that are discussed in Table 1. Respondents were asked to indicate their level of support on a five-item Likert scale. In the surveys, we also include questions to operationalise the hypotheses discussed in the previous section (Table 2). To measure *app use*, we ask respondents whether they use four different types of apps: (1) the app of their health insurance, which promises benefits in exchange for personal health data; (2) the SwissCovid app provided by the national government; (3) the app of the national railway company, and/or (4) an app for online banking. We used regression scores from principal component analysis to combine these four measures to obtain a more robust measurement of app use.

To operationalise *levels of trust*, we ask respondents to indicate the extent to which they trust the federal government (five-item Likert scale). Regarding the measurement of *issue importance*, we use four questions about issue importance—one for each policy issue (Figure 1). We asked respondents whether they believed that the issues for which we requested their propensity to share personal data for public policy—for example, preventing fraud in social insurance—were important policy problems (five-item Likert scale). To measure the placement of respondents on a *left right-scale* we use items to measure respondents' political ideology on a left-right scale in the same ways as they measured in the Swiss Election Study (Tresch *et al*., 2020) and in international comparative studies (Kriesi *et al*., 2012). Notably, we asked questions regarding respondents' positions on taxation and social spending (cf. supplementary materials for more information).

We also include several control variables. Respondents indicated how willing they were to take risks (scale from one to ten) for us to measure how they assess the uncertainty inherent in sharing personal data for public policy (cf. Nadeau, Martin and Blais, 1999). The survey also measures different levels of education (categorical variable: obligatory school, vocational training, high school, advanced vocational training, university

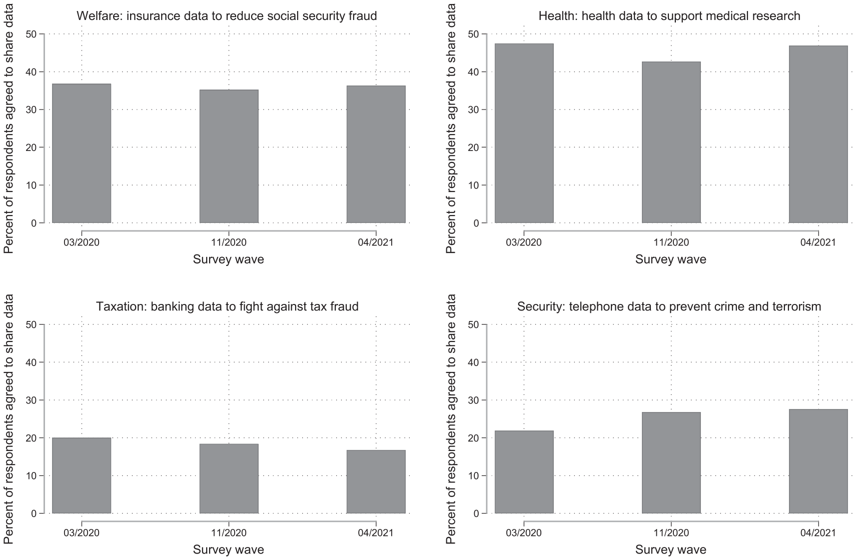

Figure 1. Agreement to share personal data for public policy.

degree) and includes variables for age, region (French- or German-speaking), and sex (female or male).

To analyse the data, we merged the different survey waves and pooled them into a single dataset, even though the respondents in the samples differ. Panel mortality was high and probably non-random and we obtained more responses for the third-panel wave. Nevertheless, this is no problem since we do not need statistical panel analyses to test our hypotheses. In the following step, we stacked the data, which means that we appended the data*set al*ong the four policy fields to create one variable that measures data sharing in the four policy fields. Prior to the regression analysis, we also standardised the data around two standard deviations to make the coefficients easier to compare. More information on the questions we posed as well as a table with the descriptive statistics of the unstandardised variables can be found in the supplementary materials to this article (see Table S1 in the supplementary materials). The data for the analyses are available online (cf. data availability statement).

All survey samples were fielded in times of the COVID-19 crisis, which makes the information of the samples largely comparable. At the same time, respondents react under conditions that are different from the pre- and post-crisis period, and this might affect the results. We discuss this point in the conclusions of the article. Furthermore, the sampling strategy of the first survey is slightly different from the second and third sample. The second and the third survey waves allow for a reasonable comparison over time as they were both fielded after the first wave of the pandemic, i.e., during the 'particular situation' once the first measures against the pandemic were taken, when the Swiss COVID app was available, and data sharing for public policy was part of the political debate. For these reasons, we use the first sample only for descriptive analyses (see section 5) and the third and second one for the regression analyses (see section 6).

Agreement to share personal data differs between policy issues

In all three surveys, respondents could indicate their consent to share their data on a five-item Likert scale. We aggregated the respondents who indicated that they somehow agreed or completely agreed to share their data for the specific policy issue (see Figure 1).

The first remarkable result is that less than 50 per cent of respondents are willing to share any of the data types for any of the policy purposes specified. Such a finding is congruent with the 2015 Eurobarometer observation that about two-thirds of respondents in various EU members states express strong privacy concerns about data sharing with private companies or public authorities. The results from the Swiss surveys show however that respondents' agreement to share their data strongly varies across policy fields and is only slightly different across survey waves (Figure 1). The data reveal that support for sharing health and social security data is higher vis-a-vis banking and telephone data. The differences across policy fields are statistically significant if we compare the survey samples for the different policy fields using paired T-tests.[3] Even when there is some variation over time, the 'ranking' of the four policy fields remains the same. Respondents are most willing to share their data for (1) health policy, followed by (2) welfare policy, (3) security policy, and (4) taxation policy.

Agreement to share personal data for public policies differs between individuals

We now turn to the results of the regression analyses. We use OLS regression models with heteroskedasticity-robust standard errors, rather than ordered logit regressions, since the OLS models have much lower values for the Bayesian information criterion (BIC) and the Akaike information criterion (AIC). Substantially, the results do not differ across model types. In addition to the above-discussed variables, we insert a binary variable that controls for the two different survey waves and a categorical variable that measures the different policy fields. Model 1 estimates the likelihood to share data for public policy including the variables that operationalise our hypotheses as well as the control variables. Model 2 adds an interaction effect between trust and issue importance. Model 3 includes the interaction between trust and policy fields. Model 4 controls for the interaction between issue importance and policy fields (Table 3).

Table 3. Linear regression models, robust standard errors in parentheses.

	Model 1	Model 2	Model 5	Model 6
Trust in federal government	**0.101*****	**0.102*****	**0.110*****	**0.100*****
	(0.006)	**(0.006)**	**(0.011)**	**(0.006)**
Importance of the issue	**0.176*****	**0.178*****	**0.176*****	**0.163*****
	(0.006)	**(0.006)**	**(0.006)**	**(0.011)**
App usage	**0.063*****	**0.063*****	**0.063*****	**0.062*****
	(0.005)	**(0.005)**	**(0.005)**	**(0.005)**
Left-right placement	0.004	0.004	0.004	0.003
	(0.006)	(0.006)	(0.006)	(0.006)
November 2020 (base category)				
April 2021	0.018**	0.018**	0.018**	0.018**
	(0.006)	(0.006)	(0.006)	(0.006)
Education	0.023***	0.023***	0.023***	0.022***
	(0.006)	(0.006)	(0.006)	(0.006)
Risk	0.007	0.007	0.007	0.007
	(0.006)	(0.006)	(0.006)	(0.006)
Age	−0.030***	−0.030***	−0.030***	−0.028***
	(0.006)	(0.006)	(0.006)	(0.006)
German-speaking (base category)				
French-speaking	−0.020***	−0.020***	−0.020***	−0.020***
	(0.006)	(0.006)	(0.006)	(0.006)
Male (base category)				
Female	−0.049***	−0.049***	−0.049***	−0.050***
	(0.005)	(0.005)	(0.005)	(0.005)
Welfare (base category)				
Health	0.078***	0.078***	0.078***	0.077***
	(0.008)	(0.008)	(0.008)	(0.007)
Taxation	−0.165***	−0.165***	−0.165***	−0.168***
	(0.008)	(0.008)	(0.008)	(0.008)
Security	−0.103***	−0.103***	−0.103***	−0.102***
	(0.008)	(0.008)	(0.008)	(0.008)
Trust in fed. gov.*Issue import.		**0.018***		
		(0.009)		
Welfare*Trust in feder. gov. (base_cat.)				
Health*Trust in feder. gov.			−0.006	
			(0.016)	
Taxation*Trust in feder. gov.			−0.027$^+$	
			(0.015)	
Security*Trust in feder. gov.			−0.001	
			(0.016)	
Welfare*Issue import. (base cat.)				
Health*Issue importance				0.069***
				(0.015)
Taxation*Issue importance				−0.013
				(0.014)
Security*Issue importance				0.007
				(0.016)
Constant	0.498***	0.497***	0.498***	0.498***
	(0.007)	(0.007)	(0.007)	(0.007)
AIC	7140.63	7139.04	7142.49	7114.48
BIC	7246	7252	7271	7243
Observations	13836	13836	13836	13836

$^+p < 0.1$, $^*p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$.

The results of the analyses show that three main factors are associated with a higher likelihood of sharing personal data for public policy (Table 3). First, when individuals consider the policy problem personally important, they are more likely to share their data. Second, if respondents hold a high level of trust in their government, they are more likely to share their data with State officials. Third, those who already use one or several (private and/or public) apps using personal data (i.e., health insurance, the Swiss-Covid-app, railway ticketing, or e-banking) are also more likely to share their personal data with the State, regardless of the type of data they share (social security, health, banking, or telephone data).

In contrast, political ideology seems no to be associated with the willingness to share data for public policy. Further analyses reveal that those leaning to the left tend to be more willing to share their social security data than those leaning to the right, however, these results are not very significant/ robust (cf. supplementary materials for these analyses). The findings also reveal that women and French-speakers are less likely to share their data for public policy. Those who are older seem to be less willing to share data for public policy. A higher level of education seems to slightly increase the propensity for data sharing. Furthermore, the findings indicate that during the third survey wave (March 2021), respondents are more likely to share their data than during the second wave (November 2020). A plausible explanation for this finding is that respondents got used to data sharing for public policy during the COVID-pandemic. The results also confirm the insight from Figure 1, which shows that compared to social security data, citizens are more likely to share their health data and less likely to share their banking and phone data for public policy. Our results remain the same if we control for respondents' cultural openness and political interest (variables not included in the analysis, in Table 3).

The interaction effects in Model 2 indicate that trust in government and issue importance reinforce each other. In other words, if citizens trust the government, they are more likely to share their data for public policy if they consider the problem to be important to them. Models 3 and 4 include interactions between the different policy fields and trust as well as issue importance. The main finding from the last two models indicates that especially those who consider health an important topic are willing to share their health data (in comparison to social security data).

In addition, we conduct sub-group analyses for some of the control variables. Firstly, we look at the differences between policy fields. The results show that the above-discussed findings are quite similar across different policy fields regarding the variables that operationalise the hypotheses we discussed. The only exception is the interaction between trust in government and issue importance. In these analyses, the effect is visible regarding the sharing of banking and phone data but not for social security and health data. The regression coefficients of the control variables indicate that educated individuals are especially likely to share their social security and banking data for public policy compared to those with lower levels of education. Furthermore, the elderly are less likely to share social security and banking data compared to younger generations. Secondly, we compare the two language groups that are included in the analysis. The results reveal that amongst French-speaking respondents the probability to share personal data for public policies increased in April 2021 compared to November 2020. In addition, amongst the German-speaking population, those with a higher level of education and a greater probability to take risks are more likely to share their data, whereas the elderly are less willing to do this. These effects are not as clearly visible amongst French-speaking respondents.

Thirdly, we compare the survey wave from November 2020 with the data from April 2021. In the April 2021 data, the interaction of trust and issue importance is particularly noteworthy. This result implies that if individuals consider a policy issue important, they are especially likely to share their data if they trust the government. The control variables also reveal that the effects of education (more likely), risk-taker (more likely), and age (elderly less likely) on data sharing are stronger for the later survey wave. We discuss the implication of this finding in the following paragraphs. Fourthly, we conduct sub-group analyses for three different age groups (18–39, 40–60, and older than 61). The results reveal a left-right polarisation amongst the oldest participants in the survey. Those who agree with policy positions that can be considered left-wing are more likely to share their data compared to those with rather right-wing positions. The youngest group of respondents was much more likely to report willingness to share their data in the April 2021 survey, and French-speaking respondents, in the youngest group, are significantly less likely to share their data.

To better interpret the results, we now turn to a graphical analysis of the results regarding those variables that we use to operationalise our hypotheses and that turn out to be statistically significant in the regression analyses. Figure 2 illustrates that the likelihood to share data increases from 14 per cent to 50 per cent between the lowest and highest levels of issue importance. Regarding trust in federal government the propensity to share data augments from 30 per cent to 50 per cent from the extreme values of the variable measuring trust. Finally, concerning app usage, the probability to share data increases from 37 to 50 per cent between the lowest and highest value for app usage. All the values are calculated with balanced values for the co-variates (Figure 1).

Our findings lend strong support to three of our hypotheses. First, citizens are more likely to share their data for the purposes of improving policy-making if they already use apps. This result supports the 'slippery slope' or 'foot-in-the door' psychological argument (van der Burg 1991), which

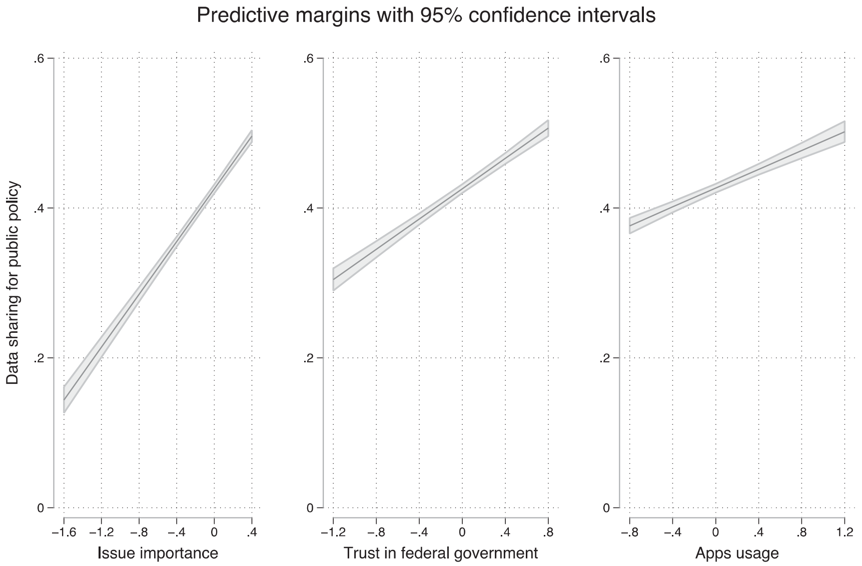

Figure 2. Predictive margins on issue importance, trust in government, and app usage.

implies that once individuals have started to use one application that requires their personal data, they are more inclined to also use other apps. Our results suggest that those who already have the habit of sharing their data also agree to do so for public policy, as expected by our fifth hypothesis. Second, our findings support the first hypothesis, according to which individuals who express higher trust in government are more likely to share their data for public policy as they do not perceive the state as a threat to their personal freedom (Bennet and Raab, 2006; Murphy *et al*., 2021). Third, the findings also show that individuals tend to share their personal data for public policy if they consider that the policy problem the data ought to help address is an important issue (as expected by our second hypothesis). This result lends support to the argument that citizens are willing to share their data if the latter helps resolve problems they consider important to their personal life, in the same way, that they support politicians who promise to address these issues (Bélanger and Meguid, 2008; Budge and Farlie, 1983).

In contrast, the models suggest that ideology does not really matter (Table 3). Only the supplementary sub-group analyses suggest that respondents who are over 60 years old are more likely to share their data if they support policy positions associated with left parties. Apart from this small effect, we do not find any significant information regarding willingness to share data for public policy.

Finally, our findings might have implications for studying how age affects readiness to share data for public policies. Previous research has focused on younger individuals' willingness to share data and pointed to the importance of trust (Murphy *et al*., 2021). Our work confirms this research and adds that readiness to share data decreases with old age especially in the survey data obtained in April 2021 and amongst the German-speaking population in Switzerland. We also demonstrate that women clearly report a lower agreement for data sharing regarding public policy. This finding might have implications for feminist privacy research (e.g., Theilens *et al*., 2021; Wyatt, 2008).

Another important graphical description underlines the findings concerning third hypothesis focusing on the interaction of personal issue importance and trust in government. Figure 3 shows that at the average level of issue importance, trust in government increases the likelihood for the data we obtained in April 2021. During the survey conducted in November 2020, this effect was not visible. This effect is a bit bigger regarding those two policy fields where the overall willingness to share data for public policy is overall low (Banking and phone data). Surprisingly, the effect is rather

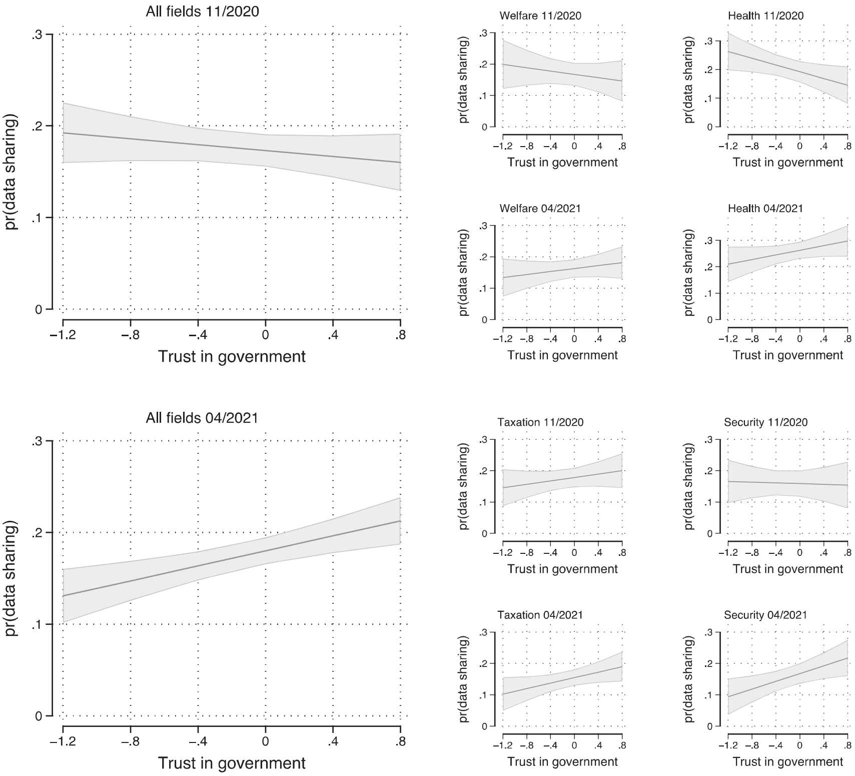

Figure 3. Average marginal effects of issue importance over trust in government (95 per cent confidence intervals).

strong for health data where it changed from a negative effect in November 2020 to a positive one in April 2021.

At this point, we can only speculate about the precise reasons for this change in attitude. One plausible explanation for this is that there was a politicisation and learning effect about data-sharing for public policy during the period between the two surveys in the sense that those who trust the government and consider the problem important are more willing to share their personal data with the government for public policy. A very hypothetical justification for this result is that between the two surveys the vaccination programmes started in Switzerland, and many citizens understood that they need to provide their data for the authorities to implement measures to lift regulations for those who are not vaccinated. The fact that being a risk-taker, highly educated, and young increases willingness to share data in this survey wave supports this argument since these groups are more likely to get the vaccine (at least amongst the young and urban population) (Léos-Torro *et al*., 2021).

Robustness of findings and limits

Our empirical analyses need to be interpreted carefully and we want to discuss four potential caveats. Firstly, it is worth highlighting that issue importance is not strongly correlated with ideology, thus legitimising the formulation of two distinct hypotheses. Nevertheless, critics could argue that the concept of 'issue ownership' (which the fourth hypothesis relies on) is multidimensional and encompasses both issue importance and policy position. Accordingly, voters perceive the party that owns an issue as the party that most cares about said issue (issue importance or policy priority) and, at the same time, as the party most able to handle the issue (policy objective or ideological policy positions) (see Walgrave *et al*., 2012, 2015). We thus re-estimate the models leaving the measure of issue importance out as a robustness check: the effect of ideology fails to become stronger (cf. supplementary materials).

Secondly, in our empirical analysis, we measure the willingness of citizens to share their data for public policy based on survey data that reports intended behaviour, but we do not measure whether individuals really share their data. This is a potential validity problem in our data. Indeed, we face a paradox that is documented by previous studies: most people express very deep concern for privacy when they fill in a survey; at the same time, when they are confronted with practical choices to share or not to share their data, mostly with private companies, they eventually accept high privacy costs to benefit from the services provided by a new app (see Martin and Nissenbaum, 2016). Nevertheless, there is a high correlation between reported app use and willingness to share data. This implies that the difference of reported vs. real behaviour regarding data sharing for public policies is probably not a major concern in our data set because respondents provide coherent information in the survey.

Thirdly, we claim to investigate the willingness of citizens to share private information with the State for the purposes of improving policymaking. We are quite confident that our results are robust for Swiss citizens, since we run consecutive surveys confirming the key findings. However, one limitation of such a research design is that the new insights we provide applies to Swiss residents only. Because privacy concerns are known to vary internationally (e.g., Pleger *et al*., 2021), the external validity of our conclusions should be addressed by upcoming studies. Indeed, we don't know whether Swiss citizens are more 'privacy preserving' than folks in other countries. In addition, we should also highlight that a Swiss idiosyncrasy might concern specific survey questions, as for instance the item about fiscal fraud. The 'banking secrecy' is traditionally high in Switzerland and privacy concerns might be thus higher than in other countries in this particular policy domain.

To ensure that our results are valid beyond the Swiss case, we use data from an Austrian survey to approximately replicate our results (Kittel *et al*., 2021). In a nutshell, regression analyses with these new data show that respondents who trust the government and use apps are most likely to share their personal data for public policy related to the COVID-19 pandemic, whereas political ideology has a weaker effect. Our analysis controls for respondents' age, education, readiness to take risks, and sex. The findings are available in the online supplementary materials.

Fourthly, we acknowledge that our survey items conflate data types with data use scenarios. This is potentially problematic since previous work has found data type and data use to have different (if sometimes overlapping) sets of expectations depending on the social context (Martin and Nissenbaum, 2016). Because our survey questions combine different data types with different policy uses, we are unable to disentangle whether it is data type, data use, or a combination of both that eventually impact respondents' judgment of data sharing acceptability. This limit should be considered when developing new surveys and comparison across policy domains. Furthermore, this last point is also relevant from a practical point of view: How is a government agency to know if it has public warrant to use one data type asked about for a different purpose?

Conclusions

This study contributes to the social science literature regarding ICT usage in public policy. Our empirical evidence shows that citizens' support for data sharing is generally low, but higher for attempts to prevent benefit fraud in social assistance and to improve health research than for efforts related to fighting tax evasion or preventing crime and terrorism. Our interpretation of this result is that citizens' willingness to give away personal data for public policy increases if they expect a personal benefit. Yet, if they perceive a potential danger from a privacy breach through policing, individuals' readiness to share their data declines. In comparison with recently published research (e.g., Wenzelburger *et al*., 2023), our study focuses on the sharing of personal data for public policy in general and examines very different contexts of personal data.

This explanation is plausible because our analyses also clearly indicate that citizens are more willing to share their data with the State if they already use apps developed by private businesses (e.g., health insurers' apps) or public agencies (e.g., the SwissCovid App) (Lupton, 2016; Lyon, 2002). In addition, respondents are more prone to sharing their data for policy-making if they trust their government (Debus and Tosun, 2021; Wynen *et al*., 2022) and if the specific policy in need of their data addresses an important issue (Bélanger and Meguid, 2008; Budge and Farlie, 1983). In contrast and quite surprisingly, party politics and ideological preferences about the targeted policy objectives less clearly predict citizens' attitudes towards data sharing.

This study opens multiple venues for further research. More specifically, the next step would be to compare respondents who use contact-tracing apps to those who do not to better control for the possible gap between real behaviour and self-reported intentions. Another extension of this research would be to include a more fine-grained measurement of trust and compare trust in different sector-specific public authorities and trust in private versus public apps (Six and Verhoest, 2017). Future research should also assess the gender dimension of attitudes towards the use of sensitive data in public policy and related differences in the perceptions of the political dimension of privacy (e.g., Theilens *et al*., 2021; Wyatt, 2008). Finally, it would be important to redo this analysis in a time beyond crisis, since our data was collected during the COVID-19 period. In this instance, it would be particularly interesting to examine whether the level of willingness to share data remains the same and if the explanatory variables maintain their power. Furthermore, it would be very interesting to conduct the same study in different countries. Switzerland's measures against the COVID-19 pandemic were much less restrictive than in neighbouring countries (Trein *et al*., 2023), which might have influenced on willingness to share data for public policy.

Finally, what are the implications of this study from a normative and practical point of view? So far, the mainstream literature on privacy protection has failed to discuss differences across policy domains in depth. However, we show that issue importance matters. Put differently, it seems that individuals' assessment of the costs and the benefits of sharing their data with State officials—specifically, the trade-off between their loss of privacy and their gains in solving important policy problems—is crucial to explaining how supportive citizens are of the use of their personal data for public policy. Our results bring policy domains back into the theoretical debate since differentiated privacy perceptions depend on the policy issue at stake. Furthermore, we show that party politics do not seem to matter that much. In contrast, trust in government is relevant in explaining preferences for the use of sensitive data in public policy. One possible explanation for this result is that the political debate is not yet strongly influenced by party politics, since parties do not yet have an intensely polarised position on the matter.

So, what could political decisionmakers undertake to increase the use of citizens' data in policy-making and service delivery? It is obviously too ambitious—and it would also be rather naïve—to develop even a tentative roadmap at this point. However, we suggest that public entities reflect on the following design principles when they elaborate a strategy to digitalise public policies and public administrations (Glassey, 2004). First, avoid a one-size-fits-all solution across policy domains. Rather, adopt a policy-specific and tailored approach. Second, instead of following a depoliticised approach, start with pilot-projects on policy issues that citizens consider high priorities, such as climate change, because data scandals around 'hidden' practices of data use (e.g., through AI) might undermine public trust in the technology (König and Wenzelburger, 2021). Trust is key for individuals' willingness to share their data for public policy, even if they consider an issue to be important. Third, target the actual users of existing apps, including apps developed and deployed by the private sector. Fourth, be sensitive of the gender gap as women are probably more reluctant to share their sensitive data with state authorities. To make our point clear: we do not at all pretend that these four design principles should be considered ultimate success factors. We only claim that they might be worth considering if policymakers want to improve the effectiveness of the delivery of public services through greater use of citizens' personal data.

Notes

1. The Eurobarometer surveys are not fielded in Switzerland. In France, 72% of respondents are concerned about their data being abused, whereas in Germany 70% are worried about them being misused.
2. For instance, see the alliance between the advanced democracies of the USA, the UK, Canada, Australia, and New Zealand, which collaborate with the digital industry, to conduct espionage and mass surveillance in European countries.
3. The results show a difference of −0.079 for insurance and health data, a difference of 0.18 for insurance and banking data, a difference of 0.09 for insurance and telephone data, a difference of 0.26 for health and banking data, a difference of 0.17 for health and telephone data, and a difference of −0.09 for banking and telephone data. All differences between policy fields are statistically significant.

Acknowledgements

We would like to especially thank Nicolas Bocquet and Martino Maggetti for extremely helpful comments regarding the revision of the paper. We also thank the attendants of the Digital Democracy Lab's Annual Meeting 2020 and the Swiss Political Science Annual Meeting in 2021 for helpful comments and suggestions. Furthermore, we thank three anonymous reviewers and the editors of the journal for their comments and support. We are grateful for financial support from the Swiss National Science Foundation (Ambizione Grant Nr.: 185963).

Disclosure statement

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

Funding

This work was supported by Schweizerischer Nationalfonds zur Förderung der Wissenschaftlichen Forschung: [Grant Number 185963].

Data availability statement

The data for the analysis in the paper is available here: https://osf.io/3y9nr/ (Open Science Framework).

Notes on contributors

Philipp Trein is Assistant Professor in Public Administration and Policy at the IEP (Institute of Political Studies) of the University of Lausanne and a Senior Fellow at the IES (Institute of European Studies) at UC Berkeley. His research interests cover comparative public policy and administration, digitalization, health policy, social policy as well as multilevel governance and federalism. The results of his work are published in leading journals of political science (e.g., European Journal of Political Research, West European Politics), public administration (e.g., Public Administration Review, Governance), and public policy (e.g., Journal of European Public Policy, Policy Sciences). His latest research project deals with the integration of artificial intelligence into public policy. More information can be found here: https://www.philipptrein.com/publications/.

Frédéric Varone is full professor of political science at the University of Geneva. His current research interests include comparative public policy, program evaluation, public sector reforms, interest groups and political elites. He has published scientific articles in major journals in political science (e.g., American Journal of Political Science, Comparative Political Studies, Governance, West European Politics) and in public policy and administration (e.g., Journal of European Public Policy, Public Administration Review, Journal of Public Administration Research and Theory). He co-authored with Michael Hill the eighth edition of the classic textbook "The Public Policy Process" (2021, Routledge).

ORCID

Philipp Trein http://orcid.org/0000-0001-6217-6675
Frédéric Varone http://orcid.org/0000-0002-5620-3291

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies*, *42*(2), 249–274. https://doi.org/10.1086/671754

Ahn, M. J., & Bretschneider, S. (2011). Politics of e-government: e-government and the political control of bureaucracy. *Public Administration Review*, *71*(3), 414–424. https://doi.org/10.1111/j.1540-6210.2011.02225.x

Bach, D., & Newman, A. L. (2007). The European regulatory state and global public policy: Micro-institutions, macro-influence. *Journal of European Public Policy*, *14*(6), 827–846. https://doi.org/10.1080/13501760701497659

Bearth, A., & Siegrist, M. (2020). Psychological factors that determine people's willingness-to-share genetic data for research. *Clinical Genetics*, *97*(3), 483–491. https://doi.org/10.1111/cge.13686

Bélanger, E., & Meguid, B. M. (2008). Issue salience, issue ownership and issue-based vote choice. *Electoral Studies*, *27*(3), 477–491. https://doi.org/10.1016/j.electstud.2008.01.001

Belle, N., Cantarelli, P., & Battaglio, R. P. (2021). To consent, or not to consent? The publicness effect on citizens' willingness to grant access to personal data in the face of a health crisis. *Journal of European Public Policy*, *28*(5), 782–800. https://doi.org/10.1080/13501763.2021.1912147

Bellucci, P. (2006). Tracing the cognitive and affective roots of "Party Competence": Italy and Britain, 2001. *Electoral Studies*, *25*(3), 548–569. https://doi.org/10.1016/j.electstud.2005.06.014

Beniger, J. R. (1986). *The control revolution: Technological and economic origins of the information society*. Harvard University Press.

Benndorf, V., & Normann, H. (2018). The willingness to sell personal data. *The Scandinavian Journal of Economics*, *120*(4), 1260–1278. https://doi.org/10.1111/sjoe.12247

Bennett, C. J. (2011). In defense of privacy: The concept and the regime. *Surveillance & Society*, *8*(4), 485–496. https://doi.org/10.24908/ss.v8i4.4184

Bennett, C. J. (2016). Voter databases, micro-targeting, and data protection law. Can Political Parties Campaign in Europe as They Do in North America? *International Data Privacy Law*, *6*(4), 261–275. https://doi.org/10.1093/idpl/ipw021

Bennett, C., & Raab, C. D. (2006). *The governance of privacy: Policy instruments in global perspective*. MIT Press.

Björklund, F. (2016). E-Government and moral citizenship: The case of Estonia. *Citizenship Studies*, *20*(6-7), 914–931. https://doi.org/10.1080/13621025.2016.1213222

Bocquet, N. (2023). The privacy-surveillance trade-off in liberal democracies. Tracing a genealogy of the data protection framework, unpublished paper.

Budge, I., & Farlie, D. (1983). Party competition – Selective emphasis or direct confrontation? An alternative view with data. In H. Daalder, & P. Mair (Eds.), *West European party systems. Continuity and change* (pp. 267–305). Berverly Hills / London: Sage.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing*, *19*(1), 7–19. https://doi.org/10.1509/jppm.19.1.7.16951

Chadwick, A., & May, C. (2003). Interaction between states and citizens in the age of the Internet: ‘E-Government’ in the United States, Britain, and the European Union. *Governance*, *16*(2), 271–300. https://doi.org/10.1111/1468-0491.00216

Ciusi, F., Fisher, S., Kayser-Bril, N., Mätzener, A., & Spielkamp, M. (2020). *Automating society report 2020*. AlgorithmWatch/Bertelsmann Stiftung.

Debus, M., & Tosun, J. (2021). Political ideology and vaccination willingness: Implications for policy design. *Policy Sciences*, *54*(3), 477–491. https://doi.org/10.1007/s11077-021-09428-0

de Goede, M. (2014). The politics of privacy in the age of preemptive security introduction. *International Political Sociology*, *8*(1), 100–104. https://doi.org/10.1111/ips.12042

Desrosières, A. (1993). La politique des grands nombres. Histoire de la raison statistique. La Découverte & Syros.

Dobber, T., Trilling, D., Helberger, N., & de Vreese, C. (2019). Spiraling downward: The reciprocal relation between attitude toward political behavioral targeting and privacy concerns. *New Media & Society*, *21*(6), 1212–1231. https://doi.org/10.1177/1461444818813372

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New Public management is dead—Long live digital-era governance. *Journal of Public Administration Research and Theory*, *16*(3), 467–494. https://doi.org/10.1093/jopart/mui057

EU. (2015). *Data protection. Special eurobarometer 431*. EU Commission.

Evens, T., & Van Damme, K. (2016). Consumers’ willingness to share personal data: Implications for newspapers’ business models. *International Journal on Media Management*, *18*(1), 25–41. https://doi.org/10.1080/14241277.2016.1166429

Fang, Z. (2002). E-government in digital Era: Concept, practice, and development. *International Journal of the Computer, the Internet and Management*, *10*(2), 1–22.

Ferguson, A. G. (2017). Policing predictive policing. *Washington University Law Review*, *94*(5), 1109–1190.

Gandy, O. H. (1993). *The panoptic sort: A political economy of personal information*. Avlon Publishing.

Glassey, O. (2004). Developing a one-stop government data model. *Government Information Quarterly*, *21*(2), 156–169. https://doi.org/10.1016/j.giq.2003.12.012

Green, J., & Jennings, W. (2012). The dynamics of issue competence and vote for parties in and out of power: An analysis of valence in britain, 1979–1997. *European Journal of Political Research*, *51*(4), 469–503. https://doi.org/10.1111/j.1475-6765.2011.02004.x

Happ, C., Melzer, A., & Steffgen, G. (2016). Trick with treat – Reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior*, *61* (August), 372–377. https://doi.org/10.1016/j.chb.2016.03.026

Hirsch, D. D. (2011). The law and policy of online privacy: Regulation, self-regulation, or co-regulation. *Seattle University Law Review*, *34*(2), 439–480.

Horvath, L., Banducci, S., & James, O. (2022). Citizens’ attitudes to contact tracing apps. *Journal of Experimental Political Science*, *9*(1), 118–130. https://doi.org/10.1017/XPS.2020.30

Jensen, P. B., Jensen, L. J., & Brunak, S. (2012). Mining electronic health records: Towards better research applications and clinical care. *Nature Reviews Genetics*, *13*(6), 395–405. https://doi.org/10.1038/nrg3208

Kittel, B., Kritzinger, S., Boomgarden, H., Prainsack, B., Eberl, J.-M., Kalleitner, F., Lebernegg, N. S., Partheymüller, J., Plescia, C., Schiestl, D. W., Schlogl, L. (2021). The Austrian Corona Panel Project: monitoring individual and societal dynamics amidst the COVID-19 crisis. *European Political Science*, *20*(2), 318–344. https://doi.org/10.1057/s41304-020-00294-7

König, P. D., & Wenzelburger, G. (2021). When politicization stops algorithms in criminal justice. *The British Journal of Criminology*, *61*(3), 832–851. https://doi.org/10.1093/bjc/azaa099

Kriesi, H., Grande, E., Dolezal, M., Helbling, M., Höglinger, D., Hutter, S., Wüest, B., et al. (2012). *Political conflict in Western Europe*. Cambridge: Cambridge University Press.

Lachat, R. (2014). Issue ownership and the vote: The effects of associative and competence ownership on issue voting. *Swiss Political Science Review*, *20*(4), 727–740. https://doi.org/10.1111/spsr.12121

Lanz, S., & Sciarini, P. (2016). The short-time dynamics of issue ownership and its impact on the vote. *Journal of Elections, Public Opinion and Parties*, *26*(2), 212–231. https://doi.org/10.1080/17457289.2016.1150285

Lee, C., Chang, K., & Berry, F. S. (2011). Testing the development and diffusion of e-government and E-democracy: A global perspective. *Public Administration Review*, *71* (3), 444–454. https://doi.org/10.1111/j.1540-6210.2011.02228.x

Leos-Toro, C., Ribeaud, D., Bechtiger, L., Steinhoff, A., Nivette, A., Murray, A. L., Hepp, U., Quednow, B., Eisner, M. P., Shanahan, L. (2021). Attitudes toward COVID-19 vaccination among young adults in urban Switzerland, Fall 2020. *International Journal of Public Health*, *66*(643486), 1–11. https://doi.org/10.3389/ijph.2021.643486

Lupton, D. (2016). *The quantified self*. Polity Press.

Lyon, D. (2002). Everyday surveillance: Personal data and social classifications. *Information, Communication and Society*, *5*(2), 242–257. https://doi.org/10.1080/13691180210130806

Macnish, K., Wright, D., & Tilimbe, J. (2020). Predictive policing in 2025: A scenario. In H. Jahankhani, B. Akhgar, P. Cochrane, & M. Dastbaz (Eds.), *Policing in the era of AI and smart societies* (pp. 199–215). Springer.

Martin, K., & Nissenbaum, H. (2016). Measuring privacy: An empirical test using context to expose confounding variables. *Columbia Science and Technology Law Review*, *18*, 176–218.

Mau, S. (2017). *Das metrische Wir. Über die Quantifizierung des Sozialen*. Suhrkamp.

Middleton, A., Milne, R., Almari, M. A., Anwe, S., Atutorno, J., Baranova, E. E., Bevan, P., Cerezo, M., Cong, Y., Critchley, C., Fernow, J., Goodhand, P., Hasan, Q., Hibino, A., Houeland, G., Howard, H. C., Hussain, S. Z., Malmgren, C. I., Izhevskaya, V. L.… Morley, K. I. (2020). Global public perceptions of genomic data sharing: What shapes the willingness to donate DNA and health data? *The American Journal of Human Genetics*, *107*(4), 743–752. https://doi.org/10.1016/j.ajhg.2020.08.023

Morse, T., & Birnhack, M. (2020). The posthumous privacy paradox: Privacy preferences and behavior regarding digital remains. *New Media & Society*, *24*(6), 1343–1362. https://doi.org/10.1177/1461444820974955

Murphy, H., Keahey, L., Bennett, E., Drake, A., Brooks, S. K., & Rubin, G. J. (2021). Millennial attitudes towards sharing mobile phone location data with health agencies: A qualitative study. *Information, Communication & Society*, *24*(15), 2244–2257. https://doi.org/10.1080/1369118X.2020.1753798

Nadeau, R., Martin, P., & Blais, A. (1999). Attitude towards risk-taking and individual choice in the Quebec referendum on sovereignty. *British Journal of Political Science*, *29*(3), 523–539. https://doi.org/10.1017/S0007123499000241

Petrocik, J. R. (1996). Issue ownership and presidential elections, with a 1980 case study. *American Journal of Political Science*, *40*(3), 825–850. https://doi.org/10.2307/2111797

Pleger, L. E., Guirguis, K., & Mertes, A. (2021). Making public concerns tangible: An empirical study of German and UK citizens' perception of data protection and data security. *Computers in Human Behavior*, *122*(106830), 106830. https://doi.org/10.1016/j.chb.2021.106830

Rider, K. (2018). The privacy paradox: How market privacy facilitates government surveillance. *Information, Communication & Society*, *21*(10), 1369–1385. https://doi.org/10.1080/1369118X.2017.1314531

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, *23*(3), 393–404. https://doi.org/10.5465/amr.1998.926617

Shapiro, A. (2017). Reform predictive policing. *Nature News*, *541*(7638), 458–460. https://doi.org/10.1038/541458a

Silcock, R. (2001). What is e-government. *Parliamentary Affairs*, *54*(1), 88–101. https://doi.org/10.1093/pa/54.1.88

Six, F., & Verhoest, K. (Eds.). (2017). *Trust in regulatory regimes*. Edward Elgar.

Theilen, J. T., Baur-Ahrens, A., Bieker, F., Ammicht Quinn, R., Hansen, M., & González Fuster, G. (2021). Feminist data protection: An introduction. *Internet Policy Review*, *10*(4), 1–26. https://doi.org/10.14763/2021.4.1609

Trein, P., Rüefli, C., & Vatter, A. (2023). *Health policy. Handbook of Swiss politics*. Oxford University Press.

Tresch, A., Lauener, L., Bernhard, L., Lutz, G., Scaperrotta, L. (2020). *Eidgenössische Wahlen 2019 – FORS*. FORS. https://forscenter.ch/selects_reports/slc-2020-00001/ (January 17, 2021).

Twizeyimana, J. D., & Andersson, A. (2019). The public value of e-government – A literature review. *Government Information Quarterly*, *36*(2), 167–178. https://doi.org/10.1016/j.giq.2019.01.001

Urbonavicius, S., Degutis, M., Zimaitis, I., Kaduskeviciute, V., & Skare, V. (2021). From social networking to willingness to disclose personal data when shopping online: Modelling in the context of social exchange theory. *Journal of Business Research*, *136*, 76–85. https://doi.org/10.1016/j.jbusres.2021.07.031

Van der Burg, W. (1991). The slippery slope argument. *Ethics*, *102*(1), 42–65. https://doi.org/10.1086/293369

Varone, F., Engeli, I., Sciarini, S., & Gava, R. (2014). Agenda-setting and direct democracy: The rise of the Swiss people's party. In C. Green-Pedersen, & S. Walgrave (Eds.), *Agenda setting, policies and political systems: A comparative approach* (pp. 105–122). University of Chicago Press.

Walgrave, S., Lefevere, J., & Tresch, A. (2012). The associative dimension of issue ownership. *Public Opinion Quarterly*, *76*(4), 771–782. https://doi.org/10.1093/poq/nfs023

Walgrave, S., Tresch, A., & Lefevere, J. (2015). The conceptualisation and measurement of issue ownership. *West European Politics*, *38*(4), 778–796. https://doi.org/10.1080/01402382.2015.1039381

Wenzelburger, G., König, P. D., Felfeli, J., & Achtziger, A. (2023). *Algorithms in the public sector*. Why context matters. *Public Administration*. Forthcoming.

Wyatt, S. (2008). Feminism, Technology and the Information Society. Learning from the past, imagining the future. *Information, Community & Society*, *11*(1), 111–130. https://doi.org/10.1080/13691180701859065

Wynen, J., Op de Beeck, S., Verhoest, K., Glavina, M., Six, F., Van Damme, P., Beutels, P., Hendrickx, G., & Pepermans, K. (2022). Taking a COVID-19 vaccine or not? Do trust in government and trust in experts help us to understand vaccination intention?

Administration & Society, *54*(10), 1875–1901. https://doi.org/10.1177/00953997211073459

Ziller, C., & Helbling, M. (2021). Public support for state surveillance. *European Journal of Political Research*, *60*(4), 994–1006. https://doi.org/10.1111/1475-6765.12424

Zimmer, M., Kumar, P., Vitak, J., Liao, Y., & Chamberlain Kritikos, K. (2020). There's nothing really they can do with this Information': Unpacking how users manage Privacy Boundaries for Personal Fitness Information. *Information, Communication & Society*, *23*(7), 1020–1037. doi:10.1080/1369118X.2018.1543442