AI & SOCIETY
https://doi.org/10.1007/s00146-024-02041-8

OPEN FORUM

Digital privacy and the law: the challenge of regulatory capture

Bartlomiej Chomanski[1] · **Lode Lauwaert**[2]

Received: 23 March 2024 / Accepted: 25 July 2024

Abstract
Digital privacy scholars tend to bemoan ordinary people's limited knowledge of and lukewarm interest in what happens to their digital data. This general lack of interest and knowledge is often taken as a consideration in favor of legislation aiming to force internet companies into adopting more responsible data practices. While we remain silent on whether any new laws are called for, in this paper we wish to underline a neglected consequence of people's ignorance of and apathy for digital privacy: their potential to encourage capture by industry interests. In particular, we argue that such laws may be at increased risk of capture because they are unlikely to be democratically responsive. We make this claim on a twofold basis: first, well-known theoretical mechanisms explaining how the absence of responsiveness leads to capture, identified in prior political science and political philosophy literature, yield the prediction that digital privacy legislation is likely to be unresponsive and thus captured; second, empirical data concerning the European Union's digital privacy laws, with a special focus on the General Data Protection Regulation, appears to confirm these predictions: the bloc's (world's?) flagship privacy protection law seems more responsive to corporate than citizen interests.

Keywords GDPR · Responsiveness · Democratic equality · Regulatory capture · Digital privacy

1 Introduction

Policy outcomes are responsive when they reflect what the citizens want. Responsiveness to what the citizens want is widely regarded as a virtue of political systems (see, e.g., Esaiasson and Wlezien 2017). While of course not every whim of the majority does, or should, become law of the land, it is nevertheless important that rulers be attentive to what the people want, and to follow those wishes, at least in some appropriately constrained manner. As Jason Brennan observes, responsiveness to citizen preferences, institutionalized through democratic procedures, is one of the cornerstones of a popular, though perhaps naive, defense of democratic politics. On this picture,

> After election[s], lawmakers pass new laws, regulations, and policies that reflect citizens' overall ideological preferences, or at least reflect a kind of compromise among all their disparate preferences; come the next election, citizens judge how well the lawmakers and other elected officials performed. If lawmakers failed to keep their promises, if they did a bad job, if they were corrupt and unethical, or if the policies they implemented (even if they were what the people wanted) produced bad results, citizens will hold officials accountable by voting against the bad performers and voting in favor of the good performers (Brennan & Landemore 2022, p. 21).

Philosophical defenses of responsiveness tend to be grounded more explicitly in its instrumental value. As Thomas Christiano and Sameer Bajaj put it, "[i]t is often argued that democratic decision-making best protects subjects' rights or interests *because it is more responsive to their judgments or preferences* than competing forms of government" (2022, np., emphasis added). Consequently, it is safe to conclude that responsiveness is an important democratic value whose presence contributes to desirable political outcomes.

✉ Bartlomiej Chomanski
b.chomanski@gmail.com

Lode Lauwaert
lode.lauwaert@kuleuven.be

[1] Department of Philosophy, Adam Mickiewicz University, Poznan, Poland

[2] Institute of Philosophy, KU Leuven, Leuven, Belgium

Published online: 10 August 2024

Against this background, we argue as follows: there are good reasons to think that people are ignorant and apathetic with regard to their digital privacy (roughly, they care and know little about how their digital data is stored, transferred, monetized, and collected). Indeed, the claim approaches the status of a truism. There are theoretical frameworks in political philosophy (due to Alexander Guerrrero (2014)) and political science (due to Pepper Culpepper (2011)) which posit that citizen ignorance (Guerrero) and citizen disinterest (Culpepper) about some policy area enable the policymaking in this area to be captured by special interests (roughly, when policymaking is captured, it becomes more responsive to special interests preferences than to the preferences of ordinary voters; we will expand upon this account in the penultimate section).

Applying these frameworks to digital privacy regulation yields the prediction that digital privacy regulation is likely to be unresponsive. We provide some evidence to think that the prediction is indeed borne out, at least as far as the European Union's General Data Protection Regulation (GDPR) is concerned. (Why the focus on that particular law? First, because it is widely considered a gold standard for digital privacy regulation; second, because researchers have studied both how it came about and what its effects are). The GDPR appears to have been a subject of intense lobbying and its effects appear to favor the entrenched market players, at the expense of newcomers. Its impact on consumers is ambivalent. This is what one would expect to see, if the law were captured, and if the Guerrero–Culpepper frameworks were on the right track.

Thus, we divide the paper as follows: in the next section, we introduce Guerrero's framework, and then argue that it is applicable to digital privacy legislation. In Sect. 3, we do the same for Culpepper's framework. In Sect. 4, we adduce (indirect) evidence that the GDPR is likely to be captured.

2 Guerrero: from voter ignorance to capture

To sharpen the focus of this paper, we will borrow the rough definition of responsiveness from Guerrero (2014), who introduces the core features of the concept as follows:

> Political outcomes are responsive to the extent that they are tied to what the people living in the political jurisdiction actually believe, prefer, or value, so that if those beliefs, preferences, or values were different, the political outcomes would also be different, would be different in a similar direction, and would be different because the beliefs, preferences, and values were different (p. 136).

In short, responsiveness is a relation between policy outcomes and voters' "beliefs, preferences, or values" and entails some form of counterfactual dependence of the former on the latter (because of that, a policy that is nonresponsive can, nevertheless, align with voter preferences). We adopt this understanding of the term in what follows.

In developing his framework, Guerrero argues that problems with responsiveness stem, to a large extent, from *citizen ignorance*. In particular, responsiveness requires the "meaningful accountability" of policymakers to voters. This is because, as Guerrero puts it,

> [i]n the absence of meaningful accountability, it would just be good fortune if the actions taken by representatives were responsive to the beliefs, preferences, and values of their constituents. Representatives would have no electoral incentive to act in a responsive way, and they would have no electoral incentive to learn what their constituents wanted (2014, p. 141).

In other words, for policymakers to be likely to act as the voters want them to act, they need to expect to be held accountable by the voters for their decisions, and expect the voters to reward (punish) them at the ballot box for (not) doing what the voters want.

To hold policymakers meaningfully accountable, citizens must be able to monitor their performance and its impact on political outcomes. But to engage in such "informed monitoring," citizens need to possess a suitably high level of knowledge about the crucial facts concerning both the policy area and the policymaking process (e.g., to determine causality and thus attribute praise and blame appropriately). The more complex the issues, the less likely the voters are to have the requisite knowledge. Thus, the more complex the issues, the less likely are policymakers to be held accountable. And the less accountable policymakers are, the less likely they are to be responsive.

In Guerrero's words:

> Meaningful accountability requires that ordinary citizens are capable of engaging in informed monitoring and evaluation of the decisions of their representatives. This monitoring of representatives can be thwarted by ignorance about what one's representative is doing ("conduct ignorance"), about a particular political issue ("issue ignorance"), about whether what one's representative is doing is a good thing in general ("broad evaluative ignorance"), or about whether what one's representative is doing will be good for oneself ("narrow evaluative ignorance"). Each of these kinds of ignorance can undermine the ability of ordinary citizens to engage in meaningful monitoring and evaluation of the decisions of their representatives. Issue ignorance and conduct ignorance make monitoring difficult or impossible. If I do not know what you are doing and have done, I cannot hold you

> accountable for it. And if I only know that you have done A (rather, perhaps, than B or C), but I have no idea what A amounts to (I know nothing about the issue for which A is a candidate proposal), or how it differs from B or C, I might as well not even know that you have done A—my ability to hold you accountable is equally impoverished. The two kinds of evaluative ignorance straightforwardly make meaningful evaluation difficult or impossible (2014, p. 140).

Guerrero further argues that the kinds of ignorance he has identified are especially likely to arise when the issues are *complex* and *technical*. As he puts it: 'If a political problem is information intensive—(a) factually complex (requiring extensive knowledge of information in order to understand the problem) or (b) technical (requiring advanced education or experience to understand and evaluate possible solutions)— then there will typically be widespread issue, conduct, or evaluative ignorance with respect to that problem' (2014, p. 147).

2.1 Ignorance of digital privacy

The problems highlighted by Guerrero are particularly acute when it comes to digital privacy regulation, such as is attempted by the GDPR. This is because, as a near consensus in the literature on digital privacy has it, ordinary people are profoundly ignorant of many of the most basic aspects of how their digital data are collected, processed, and monetized. Daniel Solove's (2012) seminal article puts the concern thus:

> (1) People do not read privacy policies; (2) if people read them, they do not understand them; (3) if people read and understand them, they often lack enough background knowledge to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various [biases] (2012, p. 1888).

The problem is not merely that people fail to acquire knowledge they could easily obtain if only they wanted to (although it is a part of the problem, to which we will return). Rather, contemporary methods of data analytics and processing involve computations so complicated as to be opaque even to experts, and thwart most attempts to predict the impact of sharing any particular piece of data. "[T]here are limits to the extent to which the outcomes of data processing are predictable," argue Lichelle Wolmarans and Alex Voorhoeve. "With the fast-evolving power of modern data analytics, it is hard to predict what privacy-relevant information can be inferred from the personal data that users provide, and to which purposes this information may be put" (2022, p. 97). In this, they are in agreement with Solove, who writes:

> The types of new information that can be gleaned from analyzing existing information [shared by the users of digital products] and the kinds of predictions that can be made from this data are far too vast and complex, and are evolving too quickly, for people to fully assess the risks and benefits involved. This state of affairs makes it very hard to assess whether revealing any piece of information will sometime later on, when combined with other data, reveal something sensitive (2012, p. 1890).

Not much seems to have changed about scholarly opinion in this matter in the intervening decade. As far as we can tell, the view that people know little about digital privacy remains, more or less, the consensus position.

So, questions about digital data and its processing are both *complex* and *technical* (in Guerrero's senses), hence "information intensive." Voter ignorance is to be expected. Therefore, if ignorance is sufficient for (the tendency toward) the absence of responsiveness, ignorance of matters concerning digital privacy is sufficient for (the tendency toward) the absence of responsiveness regarding digital privacy. That is, the electorate's values or preferences concerning digital privacy are unlikely to steer policymakers in a reliable way. In other words, laws such as the GDPR are unlikely to be responsive.

As we mentioned, responsiveness is generally considered instrumentally good, insofar as it leads to policymakers paying closer attention to the needs of their citizens (including the disadvantaged citizens). The absence of responsiveness, in turn, has been associated with anti-democratic political outcomes, strongly suggesting that it has instrumental *disvalue*. In short, when policymakers are not held meaningfully accountable by the general public, they are likely to be responsive to the preferences of *special interests instead*. Without democratic responsiveness, policy is likely to be *captured*. As Guerrero puts it,

> the absence of meaningful accountability leads to an increase in capture… If political officials … are free to take positions that are contrary to the interests of the nonpowerful—this makes the offices held by those officials more valuable, more worth controlling. Thus, as representatives become less accountable, it becomes more worth the effort to control those representatives or to control who is elected (p. 141).

In short, the route Guerrero charts from ignorance through non-responsiveness to capture is as follows: if citizens lack the knowledge and understanding of a policy area, policymakers are not held accountable; this makes it easier for special interests to influence political outcomes. Thus,

adopting Guerrero's framework predicts capture of digital privacy policy.

3 Culpepper: from voter disinterest to capture

A different mechanism leading from voter attitudes to capture has been identified by political scientist Pepper Culpepper (2011). As Culpepper argues, in situations where the public at large shows little interest in a policy area relative to other policy areas, it is the preferences of concentrated interest groups that are much more likely to be decisive in shaping policy. Metaphorically, the inattention from average voters creates a policy influence vacuum, happily filled by special interests. As Culpepper puts it,

> "the political salience of an issue refers to its importance to the average voter, relative to other political issues… Low salience political issues are decided through what I call 'quiet politics'. The … weapons of choice in quiet politics are a strong lobbying capacity and the deference of legislators and reporters toward [special interests'] expertise. The political competitors of [special interests and the policies they favor]… lack access to equivalent political armaments, so long as voters evince little sustained interest in and knowledge about an issue. … When an issue is of little interest to most voters, the press has little incentive to cover it and ambitious politicians gain little by acquiring expertise in it. *This creates an ideal political terrain for interest groups with a concentrated interest in the outcomes of the political process*" (2011, pp. 4–5; emphasis added).

Another way of making this point, also mentioned by Culpepper, concerns the differential impact of policy on individual users on the one hand, and on the companies using big data on the other. Public digital policy has a substantial impact on large companies that deal with digital data. But changes to public policy in this arena are likely to have a small influence on any individual consumer. In the parlance popularized by public choice scholars, the potential *benefits are*, thus, *concentrated* among the few largest companies; meanwhile, the potential *costs are dispersed* among millions of individuals. The corporate interests, therefore, have a much greater incentive, and a much easier time, to organize and lobby for favorable changes.

In contrast, given the low individual costs imposed by any policy change, it will not be worth the consumers' time to organize *en masse*. Lastly, the smaller the group, the harder it is to free-ride (for more on this mechanism, see Holcombe 2016). Consequently, the incentives are in place that favor special interest pressure groups in pushing their policy preferences on policymakers. Putting Culpepper's and Guerrero's frameworks together, we would venture to speculate that citizen disinterest disincentivizes informed monitoring and, thus, contributes to the absence of meaningful accountability.

We will now argue that the mechanisms identified by Culpepper are operative when it comes to digital privacy regulation, increasing the risk of regulatory capture. We start by defending the claim that people do not seem to think of digital privacy as terribly important, *relative to other issues*.

3.1 Disinterest in digital privacy

First, in experimental conditions, people tend to price their own privacy quite low. A recent study (Prince & Wallsten 2022) measured how much money consumers would demand per month in exchange for sharing various bits of more or less private data. On average, across a range of countries, the most invasive option (sharing one's bank balance) was priced at little more than the cost of a cup of coffee ($8.50 in PPP-adjusted dollars) per month (out of the countries surveyed, respondents in Germany priced their data the highest, demanding just under $15.50/month for this information). Other notable options for data sharing were priced at even less, and included browsing history ($4/month) and location data ($2/month). A different team of researchers found that even people with strong verbal commitments to the value of privacy can be easily incentivized to give up data in exchange for small rewards, like a free pizza (Athey et al. 2017).

For comparison, as economist William Rinehart (2020) estimates, social media users gain the equivalent of between $6,800 to $9,900 per year from using just three sites (Facebook, Instagram, and Snapchat), which comes down to between $567 and $825/month in 2020 dollars. Other types of digital services are valued even more highly. Measured by willingness-to-accept, i.e., by how much money people would need to be paid to stop using a service, researchers showed that users value search engines at approximately $1460/month, email at about $700/month, digital maps at approximately $300/month, and video streaming services at about $98/month (Brynjolfsson et al. 2019).

This strongly suggests that the collection of their digital data is low on the list of things people worry about, and the value they appear to assign to it is dwarfed by the value of the benefits they receive from the digital services they use. Consequently, even relatively small losses in the quality or convenience of these services would exceed gains from enhanced privacy protections, for most people.

Further, people continue using social media despite widely publicized privacy breaches, again indicating that their concern with sharing their digital private data is much attenuated. For one illustrative example, consider two pieces of evidence relating to Facebook, and the much discussed

Cambridge Analytica scandal. As the knowledge of the scandal began to spread widely, Facebook's stock price did indeed tumble, only to recover within less than a year to continue on a steady growth trajectory, as reported by journalist Anthony Mirhaydari, in the days immediately after the news of the scandal broke on mainstream media,

> Facebook shares fell more than 24 percent to a low set on March 26 [2018], losing roughly $134 billion in market value in the process. But less than 2 months later, after solid Facebook earnings reports and high-profile but uneventful Congressional appearances by CEO Mark Zuckerberg, shares had fully recouped their losses from the Cambridge Analytica scandal (2018, np.).

Moreover, the number of the platform's global monthly active users grew more or less at an unchanged rate, before, during, and after the scandal (Dixon 2023), whereas in the United States (the country arguably most affected by the whole affair), the number of users appears to have flatlined since 2016 (after a sharp rise between 2013 and 2016), with little visible change between 2016 and subsequent years (Gramlich 2021). This trend indicates that even those with arguably most cause for worry seem not to take Facebook's privacy woes very seriously.

Overall, the Cambridge Analytica story suggests that while privacy worries were, for a brief moment, being viewed with concern by markets, ordinary users of Facebook did not seem, in aggregate, to have cared all that much about the platform's privacy problems, and the potential dangers to their own private data. Nor do the investors appear to think that privacy issues threaten Facebook's short- and medium-term viability.

A similar story appears to be playing out with TikTok roughly at the time of writing. The accusation that the app engages in excessive data gathering, which came to public attention in the summer of 2022, and subsequent Congressional hearings in the US (Touma 2022), did little to stem the astounding growth in TikTok's active users into 2023, which essentially maintained past trends (Iqbal 2023). This suggests that concern with privacy plays a limited role in TikTok users' decisions whether to sign up for and stay on the platform.

As our final piece of evidence for a rather lukewarm attitude toward matters of digital privacy (more specifically, toward it being the EU institutions' job to regulate digital privacy), we offer survey data collected from a large representative sample of EU citizens, carried out by Eurobarometer. The results indicate that European voters seem to assign digital policy, in general, a low priority, relative to other areas of EU policymaking. In 2021, in response to the question, "Which of the following topics would you like to see addressed in priority by the European Parliament? Firstly?" (Eurobarometer 2021, p. 4), the option "The digitalisation[1] of European economy and society" ranked last out of 15 named options, with only 1% of respondents selecting it. When allowed to pick at least three options to choose as the EP's *second* priority, only 7% of respondents indicated digitalization among their choices, again ranking last from among the 15 named options (Eurobarometer 2021, p. 6).

This result is not a one-off. In a 2017 survey[2], a similar question, concerning the EP's priorities, the option "Creating a fair, open, and secure digital single market" (Parlemeter 2017) ranked *joint last* out of 13 named options (2% of respondents picking it) when respondents were asked about the EP's first priority, and dead last when it came to choosing up to three options as the EP's second priority (with only 6% of respondents picking it). European voters seem consistently to think that their institutions have many more important issues on their agenda than digital policy.

Overall, we take the above lines of evidence to bolster the case that people evince disinterest when it comes to their digital data and its regulation.

Plugging these findings into Culpepper's framework, we should expect that digital privacy regulation would tend toward capture by special interest. There is some evidence that this is indeed the case. Needless to say, the evidence also vindicates Guerrero's framework.

4 Is the GDPR (likely) captured?

In his critical survey of the literature on capture, political scientist Barry Mitnick (2011) has identified (by our count) six conditions that need to be met (jointly) in order for capture to occur. The first condition is that the industry must be able to control the decision-making body:

"The basic defining specification of capture is that it refers to cases in which a regulated industry is able to control decisions made about that industry by regulators and/or performances by regulators related to the industry." (p. 35).

The second is that the industry acquires benefits from these decisions:

> The industry "captures" regulatory decision-making and/or performance [when] what regulators decide and/or perform is what industry prefers they decide and/or perform. In short, industry is able to use regulation to steer benefits to itself over other potential targets of those benefits (ibid.)

[1] Due to the lack of specific questions about digital privacy and data, we use questions concerning "digitalization" or its cognates as a proxy.

[2] The date is relevant. It was in 2018 that GDPR became law.

Further, the benefits (such as "adoption of rules that favor a company or industry over competitors" (ibid.)) must be bestowed by *a public institution possessed of a monopoly on force*, they must be *substantial*, have a *long-term time horizon*, and be a *result of a stable relationship between industry and (relevant parts of the) government*. When it comes to the latter, as Mitnick memorably puts it, for capture to occur, it is essential that "the benefited party has been absorbed as a participating member of the governance system" (ibid)[3].

We label Mitnick's conditions for capture thus: the control condition, the benefit condition, the public-institution condition, the substantiality condition, the long-term condition, and the stable-relationship condition.

Definitive proofs of capture are elusive and we aspire to no such feat. We provide, instead, a list of considerations that should increase the credence in the belief that most of the criteria for capture identified by Mitnick have been met in the case of the GDPR. Specifically, we intend to show, first, that there are clear benefits to the biggest players regulated by the GDPR (in the form of rules that bestow a competitive advantage on them), thus meeting the benefit condition; second, that these benefits were the fruits of a stable relationship between industry and the EU institutions, thus meeting the stable-relationship condition; third, we will present evidence that some of the decisions about provisions of the GDPR were made as a result of lobbyist pressure, thus meeting the control condition. We take it as obvious that the public-institution condition is met.

On the other hand, it is less clear whether it can be demonstrated that the benefits are likely to be long term and substantial, but we see no reason to think otherwise.

That the stable-relationship condition has been met is substantiated by the fact that tech industry giants engage in active lobbying in the EU regarding all sorts of digital policies through both formal and informal channels; that the control condition has been met is substantiated by the fact that tech industry giants played an active role in the negotiations over the final shape of the GDPR, and were successful in influencing parts of the final legislation (specifically, we take this to substantiate the claim that industry interests are "absorbed as a participating member of the governance system" not just for the GDPR, but also other aspects of the bloc's digital policy). That the benefit condition has been met is substantiated by empirical data on the law's largely positive impacts on the biggest tech firms at the expense of smaller competitors (and perhaps ordinary users).

Of course, empirical reality is messy, and we by no means seek to suggest that every item on the industry's wishlist was adopted into the final form of the legislation (the control is not total). But even its more limited influence generates normative problems that should worry political philosophers.

4.1 Lobbying EU institutions

Below we present evidence both that Big Tech companies engage in substantial lobbying efforts in the EU, and that the outcomes of the GDPR are in important ways favorable to large market players, without at the same time offering clear benefits to the average EU citizen. These are in line with the predictions one would draw about digital policy on the basis of Guerrero's and Culpepper's general concerns about citizen ignorance and disinterest, and our conclusions that, in the realm of digital policy, citizens are ignorant and apathetic.

In line with Culpepper's framework, Big Tech appears to make substantial use of its lobbying "armaments," also in Brussels. As the report by Max Bank and colleagues (2021) finds, when it comes to lobbying in the EU, the digital sector outspends every other industry. Moreover, the bulk of the money spent comes from a handful of firms:

> Just ten companies are responsible for almost a third of the total tech lobby spend: Vodafone (€ 1,750,000), IBM (€ 1.750.000), QUALCOMM (€ 1.750.000), Intel (€ 1,750,000), Amazon (€ 2,750,000), Huawei (€ 3,000,000), Apple (€ 3,500,000), Microsoft (€ 5,250,000), Facebook (€ 5,550,000) and with the highest budget, Google (€ 5,750,000) (2021, p. 6).

The negotiations over the bloc's recent legislative initiatives concerning digital technologies (specifically, the AI Act) have also been subject to intense and apparently successful lobbying by the industry (see Schyns 2023).

In addition to formal ties, industry giants operate a "revolving door" style of recruiting its lobbyists, with the result that most of the lobbyists for Meta and Google are former government officials (LobbyControl 2022). There is little doubt that this practice helps build informal, personal relationships between regulators and the regulated industry as well.

Industry lobbying is also a well-documented feature of the negotiations over the content of the GDPR. Jockum Hildén (2019; 2021) painstakingly documents how lobbyists for industry on the one hand, and privacy advocates on the other, sought to influence the EU institutions (the European Parliament, the European Council, and the European Commission) engaged in the drafting of the law at various stages

[3] Mitnick's fuller explanation of this condition is as follows: "capture is relational and stable. In effect, the benefited party has been absorbed as a participating member of the governance system. The behavior of that system will be seen as predictable, and other parts of the government will want it to be predictable in order to provide predictable interactions on which they can depend in doing their own work" (2011, p. 35).

of the negotiation. The conclusion Hildén comes to, regarding the influence of these groups, is that:

> Both business networks and civil society organizations appear to have been quite successful. A closer look at the Commission's proposed regulation and the Parliament's and Council's amendments to the same reveal that while civil society was clearly not as well represented as business interests in the consultations, their input seems to have been taken into account to a high degree (2019, p. 207).

Consequently, while neither "side" went away with all the spoils, industry influence over the rules seems to have been significant. (Interestingly, Hildén points out that the Snowden revelations, which became widely known as negotiations over the GDPR's final text were ongoing, made the problem of privacy especially salient to voters, and gave the impetus to the privacy advocates' side; this, we think, also vindicates Guerrero's and especially Culpepper's frameworks; an unexpected boost to public salience—and, presumably, public knowledge—of the issues limited the influence of corporate lobbyists.) This suggests that business interests were able to control decisions over the law's provisions (e.g., by effecting favorable changes to items proposed by legislators themselves, or by influencing legislators to put forward favorable proposals) at least in some respects.

In any case, it seems that the industry has, through lobbying (and perhaps other means as well—see Zuboff 2019), established a relationship with all the actors responsible for crafting and enforcing European digital policy, and that it makes use of this relationship to influence, and seek to capture, the decision-makers in legislating and regulating key areas of its functioning. This should increase our credence that the stable-relationship condition and the control condition are met, both in regards to the GDPR and digital policy more broadly.

4.2 GDPR outcomes favor big tech

While there is some evidence that tech firms sometimes lobby to defang or weaken regulatory proposals flowing from the EU or elsewhere, we should not, therefore, conclude that any increase in government oversight over tech companies is contrary to the companies' interests.[4] Indeed, high-profile industry representatives themselves frequently call for more regulations. As legal scholar Anu Bradford (2020) recounts,

> While companies may not welcome all EU rules, they understand the advantages that come with regulation. The vice president for Microsoft, John Frank, emphasized that a company like Microsoft is "not trying to remain unregulated." Companies want customers to feel comfortable buying their products, and clear regulations can help accomplish that. For the same reason, the president of Microsoft recently called for the regulation of facial recognition technology in the United States. He stressed the importance of clear rules on this area of technology, which, if left unregulated, can unsettle consumers and be used "for ill as well as good." Amazon similarly called for the governments to "weigh in" after discovering an embarrassing mistake in its facial recognition technology [footnotes omitted] (2020, p. 239).

More recent examples include *Open AI's* CEO Sam Altman's (Kang 2023) and *Meta's* Mark Zuckerberg's (Zuckerberg 2020) pleas for more regulation, as well as Elon Musk's assurances that *X* (formerly *Twitter*) will happily comply with relatively stringent demands of the newly enacted Digital Services Act (Yun Chee 2022).

While, at face value, it may seem counterintuitive that large companies would want to be regulated *more*, Bradford lists a number of benefits that accrue to a regulated industry, especially to the largest, most established firms. As she puts it,

> Firms can send the markets and consumers a valuable signal by associating themselves with high standards across many areas of regulation, … [e.g.] by adhering to high environmental, human rights, or labor standards. In this way, firms can enhance their legitimacy, obtain reputational gains, and win over consumers whose values drive their customer behavior (2020, p. 240).

If Bradford is correct, then there is at least one respect in which more stringent regulations are indeed in the regulated industry's interest. It is, therefore, no surprise to see industry players taking an active role in lobbying for more government involvement in digital markets.

However, branding and reputation gains are not the only drivers of corporate behavior in this context. Also at work is an anti-competitive impulse. As Bradford clearly summarizes (without endorsing) the argument:

> The costs of complying with EU regulations are often particularly, even prohibitively, high for small- and medium-sized enterprises, while the large multinationals arguably have the resources to meet almost any standard that the EU sets. Thus, if anything, high regulatory barriers in the EU have the potential to protect and further entrench the power of already large

[4] Nor should we assume that greater regulation is more likely to safeguard fundamental rights. It is not immediately obvious why oversight by EU bureaucrats should guarantee that citizens' rights are better protected than in the context of free market competition.

> companies that can more easily afford to comply at the expense of small companies and entrants struggling to meet accumulating regulatory burdens. In the end, while big multinationals such as Facebook or Google make the headlines, the real hidden cost of [EU regulations] is borne by the small entrants who do not have the same capacity to engineer their products and services to meet the EU's demands (2020, p. 238).

The general argument sketched by Bradford seems to apply to the EU's digital policy, especially the GDPR.[5] The stringent regulations on data processing imposed by the GDPR require substantial financial outlays to meet, which tends to be easier to bear for larger businesses. This offers them an advantage over smaller rivals. Consequently, one would predict that, under the GDPR, larger (by market share) companies would fare better than smaller ones. This is what empirical data strongly suggests, in line with George Stigler's classic theory of regulatory capture according to which "every industry … that has enough political power to utilize the state will seek to control [market] entry [by newcomers]. In addition, the regulatory policy will often be so fashioned as to retard the rate of growth of new firms" (1971, p. 5). In light of a range of studies, the GDPR appears to have benefitted large digital companies by increasing their market share relative to smaller rivals, erecting barriers to entry or prompting exit of smaller competitors.

First, there are strong correlations between increased market concentration and the passage of the GDPR, as reported by Garrett Johnson (2022). In line with Bradford's claims, "[r]esearch shows that the GDPR hurt competition by creating *greater harms for smaller firms* and by increasing market concentration in the data vendor market" (p. 3, emphasis added). Gal and Aviv (2020) offer a useful summary of the key mechanisms through which the GDPR harms competition by boosting the market share of the largest tech firms. Here is a sample:

> The costs of organizing a dataset in a way which complies with the GDPR may be high and are characterized by economies of scale. Accordingly, *some small entrants* might find it unprofitable to collect data.
> The GDPR prohibits or makes it more difficult to engage in some methods of data collection, creating comparative advantages to some data controllers. For example, in their seminal article Campbell et al. (2015) showed that the need to receive a user's consent to use his data imposes transaction costs for internal data collection, whose effects fall disproportionately on less diversified or *new firms*. Both dynamics *reduce the number of potential competitors* in data collection.
> The GDPR creates uncertainty, which may impose higher costs on smaller players, and might also enable large firms to use such uncertainty strategically, limiting the sharing of their data based on broad interpretations of the GDPR. Finally, the GDPR, and especially the discussions surrounding it, could have an indirect effect on data subjects, who might be more willing to provide their data to larger, more reputable firms, or to firms with which they must interact, at least until the trust of data subjects in the actual enforcement of data protection obligations is increased. The cumulative effect of such dynamics, explored in detail below, is a decline in competition in data (and in data-based) markets (pp. 5–6, emphasis added).

Christian Peukert and colleagues (2022) report similar results, showing that in the post-GDPR world, "Google is the biggest winner in terms of market share [whereas t]he list of losers includes some of Google's competitors in the advertising market" (p. 760). The authors explain their findings by noting that.

> In data-intensive markets, large firms may have an advantage in the processing of personal data. The GDPR require[s] firms to gather user consent for using cookies and processing personal data. As long as the data stay within the firm, the firm may control its compliance risks by a firm-wide consent management system. Once data are shared with a third party, however, the firm must inform its consumers and may be jointly liable for privacy violations. Hence, the GDPR has created an environment in which data sharing within firm boundaries is less risky than data sharing across boundaries. Moreover, in line with the compliance risks, websites may choose large web technology providers over small ones because these may have more resources to weather legal challenges created by the GDPR. By choosing a large web technology provider, a website may, therefore, reduce its own compliance risk (Peukert et al. 2022, p. 764).

Finally, Rebecca Janßen and colleagues find that the increase in costs imposed by the GDPR resulted in significant reductions in innovation (proxied by app development), leading to deteriorated consumer outcomes *due to reduced market entry precipitated by the privacy law*. The researchers "estimate that the depressed post-GDPR entry rate [for app

[5] Although Bradford herself points to some evidence that industry lobbying the EU is ineffective, insofar as the industry lobbyists have no more influence on policy than other interest groups, this seems consistent with our claim about democratic inequality (interest groups' voices are more likely to get a hearing than non-organized interests' voices). Indeed, this dynamic has been repeatedly observed in the EU (see e.g., Berkhout et al. (2015). Moreover, the industry ineffectiveness is empirically disputed especially in the case of the tech sector (see e.g., Schyns (2023)).

developers] would give rise to a long-run 32 percent reduction in consumer surplus and a 30.6 percent reduction in aggregate usage and therefore revenue" (2022, p. 2).

Consequently, in line with Bradford's claims above, the GDPR *has* resulted in improving the relative position of the already hugely advantaged market participants. It also seems to have harmed consumers in at least one respect, by reducing innovation.

The above findings should increase our credence in the belief that Big Tech was indeed benefitted by the passage of the GDPR—it remains an open question to what extent these benefits are substantial and long term; however, though we would venture to guess that the major provisions of the law are unlikely to change substantially in the foreseeable future. That the benefits are thought (*ex ante*, by the recipients) to be substantial is attested to by the sheer amount of resources invested in lobbying. Thus, there is some reason to think Mitnick's long-term condition and substantiality condition are probably met as well when it comes to the GDPR.

To summarize: Guerrero's and Culpepper's frameworks predict that in the circumstances where people lack either interest in, or knowledge of, a policy area, policymakers are more likely to respond to the preferences of special interests. In the case of the EU's digital policies, it is almost a truism to say that individual voters seem mostly ignorant and apathetic. Consequently, special interests are more likely to have their preferences responded to by European policymakers.[6] In this section, we argued for the conclusion that this is actually the case for the GDPR. Given that Big Tech firms lobbied the policymakers (and were at least partially successful in their efforts), and given that the legislation resulted in competitive advantages for Big Tech, we have reason to conclude that the GDPR is at least, in substantial part, especially responsive to special interest preferences. In other words, the law is at least in substantial part captured.

The differential responsiveness evident in regulatory capture has profound normative implications. In quite a clear manner, it runs afoul of *democratic equality* (see Robeyns 2017; Christiano 2012). Industry interests having more of a say on policy direction than the mass of individual voters is a violation of the principle that the preferences of each citizen ought to be given equal weight.

Moreover, the effects of reduced competition resulting from regulatory capture tend to be bad for consumer welfare, from the slowing down of innovation to the reduced quality of existing services (for instance because the resources spent on lobbying have significant opportunity costs, and could have been used for improving customer outcomes).

4.3 Responsiveness through lobbying?

One could object to our characterization of the GDPR as undermining democratic equality; after all, it could be said, average consumers' interests *were* represented when the law was being negotiated. They were represented by civil society groups focused on privacy (Hildén 2021). So it is a mistake to say that the law is unresponsive.

This reply is unpersuasive. First, according to Hilden, industry interest groups did get at least a part of what they explicitly wanted out of the law. Second, it is not entirely clear that privacy advocates' groups' priorities actually reflect what the people want. Consider: privacy groups appear to prioritize consumer privacy, and care little about industry profits; industry prioritizes its own profits and cares little about consumer privacy (insofar as there is little to profit from protecting it). But if our arguments in Sect. 3 have been correct, the people seem to give little thought both to corporate profits and to digital privacy. So it is far from clear that their preferences align with those of the privacy advocates.

One should expect privacy advocates to place a substantially higher value on protecting digital data than an average citizen would. It is, after all, the protection of digital privacy that motivates them to go to comparatively much greater lengths than an average person to influence political decision-making. If you are willing to spend your time and effort lobbying policymakers about recondite provisions of a complex law, you probably think that whatever you are lobbying for is worth much more than the monetary equivalent of two cups of coffee per month. This means you would be willing to accept different trade-offs between privacy protection and service quality than those who do not price privacy protection that highly. Therefore, it is underdetermined whether "wins" for privacy advocates align with average citizen preferences more than the "wins" for corporate lobbyists.

One could further object: of course "the people" want greater control over, and enhanced protection of, their digital data, or would want them if they were appropriately informed. And this is what the GDPR gives them. So the law is responsive.

This, however, is a misguided way to frame the problem: the question is not whether people want more privacy protection and control *simpliciter*; rather it is whether they are willing to accept the trade-off between reduced welfare from, say, less innovation and more inconvenience on the one hand, and better-protected privacy, on the other. It is, therefore, not obvious whether the trade-offs offered by the GDPR are acceptable to most people. We cannot simply assume that digital privacy trumps other values people hold.

[6] It is important to keep in mind that, like other authors we have cited in support of our theses, we are talking here about general tendencies, rather than inexorable laws; it is, thus, consistent with our overall argument that policies contrary to industry interests get passed from time to time, or that policies include a mixture of beneficial and detrimental provisions, see e.g., Chen et al. 2022.

5 Conclusion

Guerrero and Culpepper describe mechanisms by which citizen ignorance and citizen apathy lead to anti-democratic outcomes. We have argued that these frameworks apply to digital privacy policymaking and predict anti-democratic trends in digital policy. We looked at the GDPR as a prime example of such policy, and sought to show evidence that vindicates the frameworks: there are important respects in which digital policymaking appears responsive to industry interests, rather than to citizen interests.

Acknowledgements The authors extend their gratitude to Ann-Katrien Oimann, Juliet van Rosendaal, Andrew Rebera, Stefan Rummens, Torben Swoboda, Nynke van Uffelen, Laurent Voet, and Stanislaw Wojtowicz for their detailed comments on a draft of this manuscript. We also thank the reviewer for this journal who has offered a number of insightful suggestions. Earlier versions of this paper were presented in Seattle, Leuven, Lodz, Torun, and Poznan. The authors thank the audiences for their valuable feedback. BC is grateful to ID-UB for its support.

Author contributions BC—70%; LL—30%.

Funding BC's work was supported by ID-UB under Grant 081/04/UAM/0013.

Availability of data and material Not applicable.

Declarations

Conflict of interest The authors declare no conflict of interest.

Ethical approval and consent to participate Not applicable.

Consent for publication Not applicable.

Permission to reproduce material from other sources Not applicable.

References

Athey S, Catalini C, Tucker C (2017) The digital privacy paradox: small money, small costs, small talk. National Bureau of Economic Research Working Paper Series No w23488. Available at: https://www.nber.org/papers/w23488

Bank M, Duffy F, Leyendecker V, Silva M (2021) The Lobby Network: big tech's web of influence in the EU. Brussels and Cologne: Corporate Europe Observatory and LobbyControl e.V

Berkhout J, Carroll B, Braun C, Chalmers A, Destrooper T, Lowery D, Otjes S, Rasmussen A (2015) Interest organizations across economic sectors: explaining interest group density in the European union. J Eur Publ Policy 22(4):462–480

Bradford A (2020) The Brussels effect: how the European Union rules the world. Oxford University Press, New York

Brennan J, Landemore H (2022) Debating democracy: do we need more or less? Oxford University Press, Oxford

Brynjolfsson E, Collis A, Eggers F (2019) Using massive online choice experiments to measure changes in well-being. Proc Natl Acad Sci 116(15):7250–7255

Campbell J, Goldfarb A, Tucker C (2015) Privacy regulation and market structure. J Econ Manag Strategy 24(1):47–73

Chen C, Frey CB, Presidente G (2022) Privacy regulation and firm performance: Estimating the GDPR effect globally (No. 2022-1). The Oxford Martin Working Paper Series on Technological and Economic Change

Christiano T (2012) Money in Politics. In: Estlund D (ed) The Oxford Handbook of Political Philosophy. Oxford University Press, Oxford, pp 241–257

Christiano T, Bajaj S (2022) Democracy. In: Zalta E (ed) The Stanford Encyclopedia of Philosophy. Available at: https://plato.stanford.edu/archives/spr2022/entries/democracy/

Culpepper PD (2011) Quiet politics and business power: corporate control in Europe and Japan. Cambridge University Press, Cambridge

Dixon S (2023) Facebook: quarterly number of MAU (monthly active users) worldwide 2008–2023. Statista. Available at: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Esaiasson P, Wlezien C (2017) Advances in the study of democratic responsiveness: an introduction. Comp Pol Stud 50(6):699–710. https://doi.org/10.1177/0010414016633226

Eurobarometer (2021) Defending democracy|Empowering Citizens. Public Opinion at the Legislature's Midpoint. Data Annex. Available at: https://europa.eu/eurobarometer/api/deliverable/download/file?deliverableId=80255

Gal MS, Aviv O (2020) The competitive effects of the GDPR. J Compet Law Econ 16(3):349–391

Gramlich J (2021) 10 facts about Americans and Facebook. Pew Research Center. Available at: https://www.pewresearch.org/short-reads/2021/06/01/facts-about-americans-and-facebook/

Guerrero AA (2014) Against elections: the lottocratic alternative. Philos Public Aff 42(2):135–178

Hildén J (2021) Lobby in/policy out? Assessing lobbyist influence on the GDPR. Eur Data Prot Law Rev 7(4):520–538. https://doi.org/10.21552/edpl/2021/4/8

Hildén J (2019) The politics of datafication: the influence of lobbyists on the EU's data protection reform and its consequences for the legitimacy of the General Data Protection Regulation. [Doctoral Dissertation, University of Helsinki]. Publications of the Faculty of Social Sciences

Holcombe RG (2016) Advanced introduction to public choice. Edward Elgar Publishing, London

Iqbal M (2023) TikTok Revenue and Usage Statistics (2023). Business of Apps. Available at: https://www.businessofapps.com/data/tik-tok-statistics/

Johnson G (2022) Economic research on privacy regulation: lessons from the GDPR and Beyond. National Bureau of Economic Research Working Paper Series No. 30705. Available at: http://www.nber.org/papers/w30705

Kang C (2023) OpenAI's Sam Altman Urges A.I. Regulation in Senate Hearing. The New York Times. Available at: https://www.nytim

es.com/2023/05/16/technology/openai-altman-artificial-intelligence-regulation.html
LobbyControl (2022) The revolving door – from public officials to Big Tech lobbyists. Corporate Europe Observatory. https://corporateeurope.org/en/2022/09/revolving-door-public-officials-big-tech-lobbyists
Mirhaydari A (2018) Facebook stock recovers all $134B lost after Cambridge Analytica data scandal. CBS News. Available at: https://www.cbsnews.com/news/facebook-stock-price-recovers-all-134-billion-lost-in-after-cambridge-analytica-datascandal/
Mitnick B (2011) Capturing 'capture': definition and mechanisms. In: Levi-Faur D (ed) Handbook on the Politics of Regulation. Elgar Publishing, Cheltenham, pp 35–49
Parlemeter (2017) A stronger voice. Citizens' views on parliament and EU. Part II: complete survey results. Available at: https://www.europarl.europa.eu/at-your-service/files/be-heard/eurobarometer/2017/citizens-views-on-ep-and-eu/results-annex/results-annex-citizens-views-on-ep-and-eu-201710.pdf
Peukert J, Bechtold S, Batikas M, Kretschmer T (2022) Regulatory spillovers and data governance: evidence from the GDPR. Mark Sci 41(4):746–768
Prince JT, Wallsten S (2022) How much is privacy worth around the world and across platforms? J Econ Manag Strategy 31(4):841–861
Rinehart W (2020) Consumers value Facebook to the tune of $1 trillion a year. The Center for Growth and Opportunity at Utah State University. Available at: https://www.thecgo.org/benchmark/consumers-value-facebook-to-the-tune-of-1-trillion-a-year/
Robeyns I (2017) Having too much. Nomos 58:1–44
Schyns C (2023) The lobbying ghost in the machine: big tech's covert defanging of Europe's AI Act. Corporate Europe Observatory. Available at: https://apo.org.au/sites/default/files/resource-files/2023-02/apo-nid321999.pdf
Solove DJ (2012) Introduction: privacy self-management and the consent dilemma. Harv l Rev 126:1880
Stigler GJ (1971) The theory of economic regulation. Bell J Econ Manag Sci 2(1):3
Touma R (2022) TikTok has been accused of 'aggressive' data harvesting. Is your information at risk?. The Guardian. Available at: https://www.theguardian.com/technology/2022/jul/19/tiktok-has-been-accused-of-aggressive-data-harvesting-is-your-information-at-risk
Wolmarans L, Voorhoeve A (2022) What makes personal data processing by social networking services permissible? Can J Philos 52(1):93–108
Yun Chee F (2022) EU industry chief Breton, Musk signal agreement on Digital Services Act Reuters. Available at: https://www.reuters.com/technology/eu-industry-chief-breton-meet-musk-free-speech-chips-batteries-2022-05-09/
Zuboff S (2019) The age of surveillance capitalism: the fight for a human future at the new frontier of power. Profile Books
Zuckerberg M (2020) Big tech needs more regulation. Meta. Available at: https://about.fb.com/news/2020/02/big-tech-needs-more-regulation/