Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR)

Michaela Padden & Andreas Öjehag-Pettersson

To cite this article: Michaela Padden & Andreas Öjehag-Pettersson (2021) Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR), Critical Policy Studies, 15:4, 486-503, DOI: 10.1080/19460171.2021.1927776

To link to this article: https://doi.org/10.1080/19460171.2021.1927776

© 2021 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.

Published online: 20 May 2021.

Submit your article to this journal

Article views: 2684

View related articles

View Crossmark data
Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR)

Michaela Padden and Andreas Öjehag-Pettersson

Department of Political, Historical, Religious and Cultural Studies, Karlstad University, Karlstad, Sweden

ABSTRACT
How we choose to utilize digital technology has the potential to undermine the healthy functioning of democratic systems. Surveillance practices such as the tracking, collection and profiling of our online and real-world behavior pose a direct challenge to privacy rights and democratic freedoms such as fairness and antidiscrimination. This paper aims to understand how the GDPR represents risk and, in turn, how that representation shapes protection. Using Carol Bacchi’s ‘What’s the Problem Represented to Be?’ (WPR) approach to policy analysis, we illustrate how the GDPR’s dual aims of protecting both people and the free flow of personal data exist in a state of tension and that the GDPR’s framing of ‘public interest’ privileges economic growth over individual rights. Also problematic is the assumption that people are sufficiently informed to exercise control over their data, yet are being asked to agree to practices which may undermine that very autonomy.

Introduction: the European Union’s Big Data-driven economy

Big Data is ‘real’ in the sense that the term represents relatively vast collections of data which can be indexed and correlated at high speed (Kitchin 2014). Yet it is also mythical with respect to its performative power as a socio-technical imaginary, fueled by claims to reveal ‘truth’ through correlation without necessarily accounting for causality (Rieder 2018, 91; Sætnan, Schneider, and Green 2018, 5). ‘Letting the data speak’ is a popular concept among proponents, who at times recommend abandoning the search for causality altogether, claiming that Big Data’s ability to detect patterns and predict future outcomes is sufficient (Mayer-Schönberger and Cukier 2017, 6). The ‘traction’ gained by proponents’ accounts of Big Data has seen its mythical aspects emphasized (Sætnan, Schneider, and Green 2018, 5), rendering it irresistible to companies and governments seeking to increase profits, efficiency, or to generate economic growth (Accenture Strategy 2017; OECD (Organization for Economic Co-operation and Development) 2019). In the wake of the 2008 financial crisis, the European Commission launched Europe 2020: A European strategy for smart, sustainable and inclusive growth (European
Commission 2010a), which included A Digital Agenda for Europe as one of its seven flagship initiatives (European Commission 2010b). As the Commission progressed its Digital Agenda, official communications embraced both real and mythical aspects of digital technology as vital to economic recovery, asserting in a speech entitled ‘The data gold rush’ that the ‘right algorithms’ will be the ‘magic’ to ‘help us break through the mountains of rock to find the gold within’ (European Commission 2014a). Unlocking the potential of Big Data across all sectors would pave the way for ‘the data-driven economy of the future’ (European Commission 2014a), a vision which expanded to include support for other socio-technical imaginaries such as Cloud computing, the Internet of Things (IoT), Industry 4.0, Smart Cities and artificial intelligence (AI) (European Commission 2015, EIP-SCC (European Innovation Partnership on Smart Cities and Communities) 2016; European Commission 2018).

The rise of algorithmic profiling as a new profit source in the digital economy is particularly alarming to political scientists when it is used to undermine individual privacy rights and democratic freedoms, create new categories of discrimination through the profiling of groups or interfere with political processes such as voting and elections. Algorithmic profiling is a process which aggregates data from people’s online and real-world activity to identify patterns, predict behavior and assign membership to different groups by way of inference and probability (O’Neil 2016). More specifically, profiling refers to ‘a set of technologies’ used to ‘create, discover or construct knowledge from huge sets of data’ (Hildebrandt 2008, 17). As argued by Gandy and Nemorin (2019), a key transformation in strategies of governmentality as a policy tool takes place with the use of ‘nudging’ to subtly press people into making ‘better’ decisions. Profiling is also used in marketing to ‘nudge, bias, guide, provoke, control, manipulate and constrain human behavior’ (Danaher et al. 2017, 1). Profiling, ‘scoring’ and automated decision-making systems are also used by governments in EU Member States to detect welfare and tax fraud, assess the likely truthfulness of police complaints, assist in sentencing decisions, and make predictions or trigger ‘risk alerts’ in child welfare, policing, eldercare and psychiatric services (Dencik et al. 2018; AlgorithmWatch 2019). More dystopian examples can be found in non-democratic states such as in China’s multiple ‘social credit scoring’ systems, which combine credit scores with social activity to categorize people, with significant consequences for their life opportunities (Liu 2019, 31).

The focus of this paper, however, is profiling activity conducted by private companies in relation to EU residents. In the private sector, profiling and scoring is generally facilitated by data brokers, an industry with an estimated annual turnover of more than 200 billion USD (WebFX 2020). These are the third parties or ‘partners’ to which websites commonly refer when we are asked (in the EU at least, thanks to EU regulation) to consent to the placement of tracking software (or ‘cookies’, jointly regulated by the GDPR (European Union 2016) and Directive 2002/58/EC (European Union 2002) on our devices to monitor our activity. A 2013 United States’ Senate Report on the data broking industry found that data brokers tend to operate without transparency and deliberately target users’ weaknesses, for example by scoring them in terms of their financial vulnerability or assigning them to categories such as ‘Rural and Barely Making It’ or ‘Credit crunched: City Families’, before selling these categorizations to companies such as banks for targeted marketing of their financial products (US Senate 2013, 5–6). This example was highlighted as unfair and discriminatory by the Article 29 Data Protection Working
Party, but only when a data broker has sold the consumer profiles ‘without consumer permission’ (Article 29 Data Protection Working Party, 10). What is problematic here is that these practices may still have unfair and discriminatory effects even when carried out with consent and as permitted under the GDPR.

Terms such as ‘surveillance capitalism’ (Zuboff 2019) and ‘platform capitalism’ (Srnicek 2017) have been applied to these new business models where algorithmic profiling is a central feature. As EU residents were committed, wittingly or otherwise, to the data sharing demands of platform capitalism, removing barriers to trust was seen as important given that ‘lack of trust in the online environment is meanwhile seriously hampering the development of Europe’s online economy’ (European Commission 2010b, 12). Trust was brought into even sharper focus by Edward Snowden’s 2013 revelations of mass surveillance of individuals’ electronic communications and ‘hidden complicity’ between government agencies and private providers, which provided new ‘public relations challenges’ in responding to the public outcry (Zuboff 2019, 385). The European Commission’s response was to reinforce the need for safeguards so that ‘people can trust big data and seize online opportunity’ and reap the economic benefits (European Commission 2014b, 3):

Many of us were shocked by the recent revelations of online spying, and invading privacy . . . .
But, serious though this issue is, our answer cannot be extreme. For one thing, it would be dangerous, as we turn our backs on a huge digital opportunity. Like the huge economic and social innovations of big data; it would be a disaster to turn those down, and we can’t afford that (European Commission 2014b, 2).

If economic interests had hitherto thwarted privacy interests in the reform of data protection regulation, revelations of mass surveillance increased attention given to privacy issues and strengthened the influence of privacy advocates in the drafting of the Regulation (Rossi 2018). Ultimately, the GDPR, which came into force in May 2018, can be seen as the product of struggle between competing economic and rights interests (Bernt 2015).

The GDPR is claimed to protect us, yet how? To help answer this question, we analyze the GDPR by mobilizing Carol Bacchi’s ‘What’s the Problem Represented to be?’ (WPR) framework. This well-established approach to critical policy studies recognizes how we are governed through problematizations rather than problems (Bacchi 2009). In short, by looking at policy solutions we can elicit what it is that the underlying problem is considered to be: ie. the ‘problem representation’. By analyzing the GDPR’s policy solutions we can better understand how policy problems are represented in the Regulation and thereby shed light on the GDPR’s mechanisms of governing. In so doing, we identify discourses at work in the Regulation which act to shape conceptions of ‘risk’ and thereby delimit our possibilities for ‘protection’ from the outset. We examine broader discursive trends in the GDPR and related European Commission documents, which can illuminate trends in meaning-making around contested concepts such as values presented as rationales for data protection policy. Given the implications of practices such as profiling and algorithmic decision-making for fundamental rights and democratic freedoms, we consider this an important inquiry and one which can add to debate over the extent to which such practices should be enabled by regulation. In this
paper, we will firstly review some of the main literature concerning the GDPR; secondly, outline the WPR approach; and thirdly, present our analysis and discussion.

**Literature overview**

GDPR literature exists in clusters which often intersect. Computer science, for example, tends to focus on the feasibility and design of the GDPR’s proposed technical solutions to data protection risks, including privacy-enhancing technologies (Patrick and Simone 2017), the technical limits of privacy protection, such as whether it is genuinely possible to ‘opt out’ of cookies to avoid being tracked (Sanchez-Rola et al. 2019), ‘dark patterns’ (Fritsch 2017; Nouwens et al. 2020) or the effects of the GDPR on App privacy (Momen, Hatamian, and Fritsch 2019). Consumer law is interested in topics such as consumer control (Van Ooljen and Vrabec 2019) and the role of the GDPR in uncovering discriminatory practices such as personalized pricing (Zuiderveen Borgesius, Frederik and Joost Poort 2017). Business literature is more interested in ‘tapping the potential of big data’ (Engels 2017) or the Regulation’s potential to stifle innovation (Renda 2017). Literature in other fields, such as the health sciences, can cover wide ground from the extent to which privacy policies comply with the GDPR (Mulder 2019) to how Big Data can improve health outcomes. However, the reliance upon moral arguments to promote the benefits of Big Data in healthcare can be at the expense of privacy, according to Snell, who argues that ‘privacy and autonomy become silenced when contrasted with the moral principle of health’ (Snell 2019). This paper is best situated in an emerging body of literature which takes a critical approach to the politics and policies of Big Data (Sætnan, Schneider, and Green 2018) and which focuses on broader societal discourses relating to the GDPR’s key provisions (Bergemann 2018). The socio-technical imaginaries of European Commission policies to promote a ‘digital future’ and the growth of ‘Big Data’ as ‘an almost religious following’ are also related to our mode of enquiry (Rieder 2018, 90). More broadly, we are interested in the politics of algorithms (Pasquale 2015; Leese 2014; O’Neil 2016; Bellanova 2017) and the effects of technological change through the lens of surveillance (Lyon 2003; Bigo 2012; Matzner 2018; Gandy and Nemorin 2019; Zuboff 2019; Monahan and Wood. 2018). This paper also draws on the work of critical legal scholars (Koops 2014; Lyskey 2015; Daly 2016), who have written extensively about the EU’s data protection regime and power imbalances between users and controllers. Legal scholarship in areas such as algorithmic profiling (Hildebrandt 2008, Mann and Matzner 2019), group profiling (Mittelstadt 2017), the effectiveness of ‘notice and consent’ in relation to predictive analytics (Mantelero 2014), the ambiguity of the principle of ‘fairness’ in the GDPR (Malgieri 2020) and legal interpretation of the scope of risk in the GDPR and its role in relation to the principle of accountability and compliance (Demetzou 2020), is also valuable to us in our endeavor to identify problem representations in the Regulation.

**What is the problem represented to be?**

This study takes a ‘What is the problem represented to be?’ (WPR) approach to analyzing the GDPR and other key documents surrounding its inception and installation. Developed by Carol Bacchi, the WPR approach is a poststructural analytic strategy
which allows for the interrogation of policies with respect to how they constitute the problem(s) they propose to solve Carol Bacchi (2012, 1). Within these problem representations are constructions of reality to which a policy responds. The ‘claims to truth’ built into these representations underpin the practices arising out of them which, in turn, ‘govern’ us (Rabinow in Bacchi 2012, 3). According to Bacchi and Goodwin, every policy solution harbors a ‘problem representation’ with its own set of assumptions about what constitutes reality (2016, 14–16). Studying ‘problem representations’ in public policy can expose beliefs, assumptions and discourses at their core: ‘it becomes possible to probe underlying assumptions that render these representations intelligible and the implications that follow for how lives are imagined and lived’ (Bacchi and Goodwin 2016, 6). Thus, how a policy presents the ‘reality’ of the situation (i.e., the implicit causes of the problem) will have consequences for how we live our lives, which Bacchi describes as ‘lived effects.’ After identifying the problem representation and its assumptions in a WPR analysis, it is then possible to understand what is omitted or even silenced by the identified problem and the ‘reality’ it creates. By attending to ‘silences’, one can then imagine alternative solutions given a different set of preconceptions (Bacchi and Goodwin, 2016).

The paper draws particular attention to the discourses which inform the GDPR and shape its ‘reality’. Discourses are understood to be knowledges that form part of a cultural and historical trajectory, which will shape the limits of what are conceivable and conceivable notions of protection when responding to new applications of technology. For example, in the case of the GDPR, how broader, undefined concepts such as ‘public interest’ are conceived will shape how the GDPR is interpreted, applied and enforced. A WPR analysis examines policy responses and highlights how, with a particular response, a specific ‘problem’ is produced. This type of analysis opens up the possibility of rethinking the policy in question. How, for example, are subjects constituted in proposals to ‘protect’ them? What are ‘data subjects’? What rights are highlighted and how are they balanced? Why are rights ‘respected’ in proportion to ‘economic and social progress’ as opposed to being considered non-negotiable?

A WPR analysis involves a number of steps, starting with the identification of the problem representation(s) in a specific policy, followed by probing the presuppositions or assumptions which underlie this representation and how they have come about (Bacchi 2009). Following from that is the question of what is left unproblematic or silent, which aids exploration of how the problem might be thought about differently. Bacchi insists that it is important to examine the effects or implications of identified problem representations. She outlines three kinds of effects: ‘discursive effects’, which highlight how selected discourses shape the argument; ‘subjectification effects’, which look at how subjects are constituted in specific proposals; and ‘lived effects’, being how we materially experience the ‘real world’ effects of policies arising from the problem representation underlying the policy and how or where has this been produced (Bacchi and Goodwin 2016, 20). Finally, in a confrontational move, Bacchi’s method requires applying this list of questions to one’s own problem representations, which in our case would be the ‘problem’ of surveillance and profiling as a risk to democratic freedoms.

This study involved coding the GDPR on the basis of Bacchi’s steps where we identified problem representations in the GDPR and their expression in European Commission documents, their historical context, what is left unproblematic and how
the problem might be thought about differently. Although we followed the steps of the WPR approach in our coding of the material, we have presented the analysis thematically. We consider risk to be a key theme, given the Regulation’s dual aim to protect people from risks to their fundamental rights and freedoms and to protect data from risks to its free movement. Risk is also significant to our analysis as a governing rationality:

There is no such thing as risk in reality. . . . Risk is a way, or rather a set of different ways, of ordering reality, of rendering it into a calculable form. It is a way of representing events in a certain form so they might be made governable in particular ways, with particular techniques and particular goals (Dean 2010, 206).

We will now look at the GDPR’s problem representations of risk as understood through the Regulation’s policy solutions of protection. We note that although our study involves a number of legal texts, our argument is not a legal one, but instead utilizes discourse analysis as a methodology to understand how the GDPR constructs meaning, specifically of those contested terms which it counts among its aims.

**Analysis**

Having outlined the WPR framework we now turn to our analysis. We identified three main problem representations of risk in the GDPR: (1) risks to personal data of a lock and key variety, concerned with implementing the necessary technical protections to ensure that data is processed with ‘security and confidentiality’ and that information is only provided to those granted access (Recital 29, Article 25, Article 32); (2) risks to people, perceived as infringements of social and legal mutable norms, such as ‘fundamental rights and freedoms’ (Article 1), ‘fairness’, (Article 5), ‘well-being’ (Recital 2) and the ‘public interest’ (Article 6), which can be overlapping, ambiguous, subject to qualification, open to interpretation and/or changeable over time; and (3) risks to the economy, presented in the GDPR as risks to the ‘free flow’ of data (Recital 6, Article 51) or ‘divergences hampering the free movement of personal data’ (Recital 13) which need mitigating to ‘allow the digital economy to develop across the internal market’ (Recital 7). In the following analysis, we present these three main representations of risks and delve into the often complex and conflicting ways they are constructed in the GDPR. Following the WPR approach, we also describe what we argue are silences and gaps in the GDPR in terms of how it represents certain risks, specifically those connected to more abstract values and subject to change over time.

Within these three conceptions of risk are three main targets of ‘protection’: (1) ‘personal data’; (2) people (‘natural persons’); and (3) the economy. ‘Personal data’ is defined as ‘any information relating to an identified or identifiable natural person’ who is also the ‘data subject’ (Article 4). This is important in relation to profiling, which we will take up later under the section ‘silences and gaps’, given that non-personal data (not covered by the GDPR) can be used to create profiles of groups (Koops 2014, 257) and that profiling can still occur based on anonymized data (Mann and Matzner, 2019, 2). A further complication is a lack of consensus as to whether or not the profile itself, which is ‘new’, inferred information, is ‘personal information’ (Mann and Matzner 2019, 3).
Although the language of the GDPR at times suggests that people and the economy are compatible as targets of protection, we argue that they exist in a state of tension. This tension is not new but can be traced to discussions around data protection policy in the 1970s, when a much clearer division of interests could be seen between business and civil rights in the privacy versus free movement divide. We therefore begin with a brief genealogy of the emergence of the data protection principles adopted in the GDPR to underline how the target of protection appears to be drifting over time, in what appears to be a move away from privacy as a key source of human well-being essential to democratic freedoms and toward a privileging of economic well-being. This move is not as clear-cut as a direct shift away from privacy, but rather a struggle between dual, yet linked, objectives (Lynskey 2015, 46). Although free movement and rights may stand on an equal legal footing (Lynskey 2015, 62–70), the discourse at times suggests a tilting in favor of the economy over privacy. Whilst our focus here is on the economic vs privacy divide, it is worth noting other contested terms such as ‘security’ (Recital 2), or more specifically ‘public security’ (Article 2), are put into play by the GDPR as factors which also support a shift away from privacy (Bigo 2012; Bigo et al. 2013; Matzner 2018; Strauß 2018).

**A brief genealogy of people and their data: targets of protection in conflict**

The GDPR identifies two main vulnerabilities, which arise when processing personal data. These are identified in the Regulation as being, on the one hand, the risks posed to people (‘natural persons’) when their personal data is processed (Recital 2) and, on the other, the risk to economy when the ‘free movement’ of that same data is prevented (Recital 6, Recital 9). The tension between these dual aims was arguably more pronounced in debates of previous decades when economic growth was less dependent on data flows and privacy not so easily traded for a free service like a web browser or the health of the economy. As economic prosperity is increasingly tied to the easy circulation of data, the alignment of personal well-being with personal data circulation starts to become thinkable. This development favors a distancing of privacy as a central tenet of personal well-being, given that privacy protections can threaten the free flow of personal information. By tying both ‘protection’ and ‘free movement’ to the mast of ‘economic and social progress’ (Recital 2), the GDPR attempts to reconcile two concepts which have, historically, been cast in a much harsher light of opposition.

The digitization of hard copy information traditionally stored in filing cabinets generated increased interest in new types of security suited to electronic storage, which also presented new possibilities for automated processing:

Among the reasons for such widespread concern are the ubiquitous use of computers for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically dispersed locations and enables the pooling of data and the creation of complex national and international data networks (OECD 1980).

The ‘data protection principles’ developed by the OECD in the 1970s were hoped ‘to prevent what are considered to be violations of fundamental human rights, such as the
unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data’ (OECD 1980). In negotiating the principles, which took around two years, balancing the demand by business interests for ‘freedom of information’ with civil liberties was already described as ‘urgent’ at the time, as well as difficult to resolve (OECD 1980):

Numerous official reports show that the problems are taken seriously at the political level and at the same time that the task of balancing opposing interests is delicate and unlikely to be accomplished once and for all (OECD 1980).

If people were in ‘urgent’ need of ‘protection’ from ‘ubiquitous’ surveillance already in the 1970s then the explosion of computer use in the 80s and 90s made this even more pressing. The 1995 Data Protection Directive (European Union, 1995) reinforced the data protection principles set out in the OECD’s 1980 Guidelines. Like the GDPR, the 1995 Directive also aimed to guard ‘the fundamental rights of individuals’ at the same time as facilitating the ‘free movement of such data’ to ensure ‘the functioning of the internal market’ and ‘the free movement of goods, persons, services and capital’ (European Union 1995, Recital 2). Reflecting on the OECD Guidelines some thirty years after their implementation, the former Chair of the Expert Committee responsible for their formulation, Michael Kirby AC CMG, considers the ‘ultimate economic question’ for policy makers in determining the usefulness of the Guidelines for the future: Whether the ‘economic utility of attempting to impede TBDF [transborder data flows], so as to protect attributes of individual privacy, outweigh the marginal costs involved in any such interference in the operation of TBDF’ (Kirby 2011, 12). Although the technologies may have changed since Justice Kirby oversaw the Committee’s debates of the 1970s, the business-privacy divide which he adjudicated in order to produce the Guidelines remains evident in today’s GDPR.

**Problem representation 1: lock and key risks to personal data**

The first of the GDPR’s three main problem representations is the risk to personal data. That is, risk to ‘bits and pieces’ of information or ‘identifiers’ such as ‘a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’ (Article 4(1)). We will refer to this as the **lock and key** conception, given the implication that these refer to specific facts or quantifiable representations of a person, access to which may be authorized or denied, and which can be specifically targeted in a technical response. The GDPR’s solution to problems of the lock and key variety are a suite of technical rules and specifications designed to corral or secure specific bits and pieces of information to prevent things such as their ‘loss, alteration, unauthorized disclosure’ or ‘damage’ (Article 83). The GDPR has adopted many of the OECD’s data protection principles, including ‘purpose limitation’, ‘data minimization’, ‘accuracy’, ‘storage limitation’, ‘integrity and confidentiality’ and ‘accountability’ (Article 5) as well as the goal of increased control by individuals over their data (Recital 68). However, although the principles may remain desirable, it is difficult to reconcile data minimization or increased control with increased demand for the use of Big Data analytics and the high uptake of smart technologies at a time when
‘more personal data is currently being processed than at any other time in history’ (Lynskey 2015, 1–2). Koops argues along similar lines, claiming it is ‘folly’ to look at the world today and claim that ‘data minimization’ exists (Koops 2014, 256).

‘Technical and organizational measures’ (Article 5) such as ‘data protection by design and data protection by default’ (Article 25) used to provide lock and key protections are more straightforward when protecting identifiers such as birthdates and banking information, but more difficult when called for to protect values such as ‘fairness’ (Recital 71), or ‘rights and freedoms’ (Recital 78). Technical solutions are especially problematic in relation to policy goals such as ‘public interest’ (Recital 46), which is also a legal basis for data processing (Article 6(1)(e)), yet which is a contested notion in public policy more generally and open to appropriation and power struggles (Feintuck 2004). In line with the WPR approach, eliciting current understandings of key terms such as ‘public interest’ will shed light on the GDPR’s likely interpretation by EU Member States, the CJEU and the European Data Protection Board (EDPS), and its lived effects.

Problem representation 2: risks to mutable norms and values

The second conception, or rather set of conceptions, of risk, are more amorphous, involving the ‘risks’ of data processing to ‘the well-being of natural persons’ (Recital 2) and ‘fundamental rights and freedoms’ (Article 1, Article 24(1)). Risk may also arise if data is not processed when it is in the ‘public interest’ to do so (Article 1(e)). As a guiding principle, the general purpose of data processing should be ‘to serve mankind’ (Recital 4). We refer here to these (moving) targets of protection as mutable norms, given that they are deceptively familiar yet undefined and open to interpretation across disciplines of law, politics, economics and psychology, and tend to be shaped by those with forms of authority (Feintuck 2004, 33). Fundamental rights and freedoms are perhaps more stable concepts given their codification in law, yet, in the absence of any ‘objective moral order,’ are still open to change (and amendment) over time, even if this change is slow and barely perceptible (Goble 1959).

Easily glossed over given its self-evident worthiness, ‘public interest’ is a legal basis for the processing information under the GDPR (Article 6(e)) but is never strictly defined. Some guidance is provided, for example, that processing based on ‘public interest’ may include ‘humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters’ (Recital 46). ‘Public interest’ may also include ‘an important economic or financial interest of the Union or of a Member state, including monetary, budgetary and taxation matters, public health, and social security’ (Article 23(e)). The concept is not fixed and has been shown to be shaped by power struggles (Feintuck 2004). For example, as the findings of De Bruycker’s study demonstrate, EU elites ‘predominantly address public interests when policy processes are salient to European citizens and crowded with civil society groups, but remain silent about public interests on policies that attract abundant business lobbying’ (De Bruycker 2017, 605). They are thus more likely to succumb to ‘regulatory capture’ by economic power (Daly 2016, 37). An example of the mutability of ‘public interest’ can be seen in other policy areas, such as EU Merger Regulation, which is primarily concerned with ensuring effective competition and preventing unfair concentrations of power. In recent times, however, ‘public interest’ has
been used by politicians to overturn blocked mergers and allow them to proceed on the basis of economic benefits such as job creation (Budzinski and Stöhr 2019). Finally, the self-evident worthiness of ‘public interest’ is likely to become less so in societies characterized by increasing polarization, which has been shown, ironically, to be heightened by ‘recommender algorithms’ used by streaming services such as YouTube and which are based on user profiles (Cho et al. 2020). This brings us to the third problem representation, that of risk to the economy.

**Problem representation 3: Risk to the economy**

The third problem representation in the GDPR is the risk posed to the economy should the free flow of data be stymied. The right to data protection is not absolute but balanced against other rights, such as those specified in the Charter of Fundamental Rights of the European Union (European Union, 2012) and those in the European Convention on Human Rights (ECHR) (Council of Europe, 1950), an international treaty to which EU Member States are also signatories. The right to data protection is also balanced against data’s ‘function in society’, framed here as the general interests of mankind:

The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality (Recital 4) [emphasis added]).

It is therefore critical to ascertain the meaning of mutable terms such as ‘public interest’ and what it actually means to ‘serve mankind.’ As both ‘problem representations’ and contested concepts, the meaning of these terms as constructed in data protection discourse will have ‘real’ or ‘lived effects’ (Bacchi and Goodwin 2016, 6). ‘Public interest’ is specified in the ECHR as a justification for a public authority’s interference with a person’s privacy, and includes ‘the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’ (Article 8). If ‘balancing’ tips in favor of ‘public interest’ characterized by the economic interests of society, this may diminish the protection afforded other rights, such as ‘the right to respect for private and family life, his home and his correspondence’ (Article 8).

Recital 2, for example, emphasizes the economic aspirations of the EU, among others, to which it marries personal well-being:

This Regulation is intended to contribute to the accomplishment of an era of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons (GDPR Recital 2).

Public interest is presented here as a robust economy: a strong economic union among Member States as well as stronger economies within the union, as well as economic progress. The colocated of economic progress and stronger economies with the ‘well-being of natural persons’, implies a connection between the two. Equating public interest with economic progress supports the development of a digital economy which relies upon the ‘free movement’ of personal data. The interests of business are thus supported
by both the framing of public interest and individual well-being in terms of economic prosperity. A conceptualization of well-being as including a person’s economic health serves to lessen the tension between the GDPR’s dual aims of protection and free movement. When risk to our well-being is framed more along the lines of risks to our civil rights, as it is in moments of crisis (eg. Snowden and Cambridge Analytica), then this tension is perceived as more intense. When our well-being is aligned with the success of digital industries, then their success begins to be equated with the public interest and this tension begins to dissolve, resulting in the downgrading of privacy as a public good. This move, combined with post-911 security discourse (Bigo et al. 2013), helps to shift the notion of public interest away from privacy and civil rights toward a conception aligned with economic progress, economic freedom and securitization.

Equating generic concepts such as ‘well-being’ and ‘public interest’ with economic security helps to downgrade the concept of privacy in proportion to other rights. This is happening both implicitly in the linking of ‘well-being’ to economic prosperity, and explicitly, such as in Article 16 of the Charter of Fundamental Rights of the European Union, which upholds ‘the freedom to conduct a business’ (European Union 2012). In announcing A Vision for Europe, the implication was made that invasions of privacy are not as ‘dangerous’ as turning down the economic benefits of the internet (European Commission 2014b). The meaning ascribed to these more general principles influences the extent to which one considers the dual aims of ‘protection’ and ‘free movement’ to be in conflict: how we conceive of ‘well-being’ will affect how we view the GDPR’s aim to ‘contribute to the accomplishment . . . of the well-being of natural persons’ (Recital 2). If a functioning economy is considered key to personal ‘well-being’ then this will more likely produce a policy solution prioritizing ‘economic growth’ over human rights when ‘balanced against other fundamental rights, in accordance with the principle of proportionality’ (Recital 4). The ‘scale of the collection and sharing of personal data’ is presented by the GDPR as by-product of ‘technological developments’, as technology is used by the private and public sector ‘in order to pursue their activities’ (Recital 6). The movement of personal data is thus presented as a natural, unavoidable side-effect of technological progress, rather than a choice with consequences, yet just because technology allows for the performance of a particular action does not mean it should be done (Tene and Polonetsky 2014, 83).

Silences and gaps

The WPR approach prompts us to ask if the policy ‘problem’ can be conceptualized differently. Doing so can help identify ‘silences’ or ‘gaps’ in the problem representation and its solutions (Bacchi and Goodwin 2016). If, for example, the GDPR were to privilege the notion that the psychological health and well-being of people is at risk the more their actions, transactions, associations, journeys or website searches are recorded and retained for profiling, then we could probably expect a different policy solution to one which enables us to consent to ubiquitous surveillance. If concepts like well-being were instead tied to ‘freedom from constant monitoring’, or ‘freedom from mass surveillance’, we would arguably see a solution which prohibits the collection, retention, sharing and profiling of certain types of information for certain types of purposes at all. We now discuss some the GDPR’s ‘silences’ around profiling, consent and power asymmetries.
Profiling, consent and power asymmetries

The GDPR defines profiling as:

any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Article 4(4)).

Related processing activities include people being ‘tracked’ online, monitoring behavior, and using this information to profile a person to predict ‘personal preferences, behaviors and attitudes’, and potentially make decisions about them based on these predictions (Recital 24). Despite an initial impression that the GDPR will address the broader ‘normative challenges’ of profiling, this is not the case (Koops 2014, 257). Based on the GDPR’s policy solutions, ‘profiling’ in itself is not a central problem representation in the GDPR, given that the GDPR actually legitimizes profiling by giving it several legal bases (Article 6). Profiling is lawful if it meets one of several conditions, such as the ‘consent’ of the data subject (Article 6(1)(a)) or is in the ‘legitimate interests’ of the controller (Article 6(1)(f)), which can include ‘direct marketing’ (Recital 47). Risks associated with profiling are recognized only to the extent that ‘data subjects’ are afforded certain protections, otherwise profiling may proceed. In addition to principles of ‘lawfulness, fairness and transparency’ (Article 5), the ‘data subject’ should be ‘informed’ of the existence of profiling (Recital 60), given a right of access to the data collected about them, explained the ‘logic involved’ and any ‘envisaged consequences’ of automated decision-making based on the profiling (Article 13(2)(f); Recital 71). However, the data subject must also ‘specify the information or processing activities to which the request relates’ (Recital 63), which can prove an impediment in this process if the person cannot name them.

A person has the right not to be subject to a decision ‘based solely on automated processing, including profiling’ (Article 22), but the strength of this provision is weakened by the term ‘solely’, given uncertainty around the extent of human intervention necessary to render it inapplicable (Veale and Edwards 2018, 400). Although consent is intended to give people ‘control’ over their data (Recital 7), it has been argued to be an unsuitable legal basis for data processing given that people generally tick consent boxes for the sake of convenience and do not have the time to read and digest complex privacy agreements (Koops 2014, 3–4; McDonald and Cranor 2008). In terms of a WPR analysis and the identification of ‘subjectification effects’, our constitution as subjects is problematic here: We are assumed to be free, rational, autonomous and sufficiently informed to consent to the sharing and processing of our information, yet in doing so we may be agreeing to profiling practices which, if as effective as claimed, may undermine the preconditions necessary for legal consent or expose us to discrimination or manipulative practices.

Requirements that data subjects be informed of certain data processing purposes (Recital 60) or have the right to access information about them (Article 15) aim to address information asymmetries and are in keeping with the principle of transparency (Article 5). Yet addressing information asymmetries should not be confused with addressing power asymmetries. As argued by Daly, EU regulation governs private concentrations of power which hamper individual autonomy, it does not set about dismantling
them (Daly 2016, 1): ‘EU regulation does not address fully the negative impact that concentrations of private economic power have over the free flow of information online and thus Internet users’ autonomy’ (Daly 2016, 9). Power asymmetries undermine the idea that consent is freely given and that the consumer, faced with a ‘take it or leave it’ privacy notice from a platform giant, has little or no room for negotiation (Bergemann 2018, 115). The constitution of the ‘data subject’ as an identifiable person imposes a further possible restriction in accessing information, given a lack of agreement about whether profiles, which are created by companies, even count as ‘personal data’ (Mann and Matzner 2019, 2).

Group profiling is another silence of the GDPR, given that group profiles are often based on anonymized data, and therefore not covered by the GDPR’s definition of ‘personal data’ (Mittelstadt 2017, 478). The focus of EU regulation on the ‘data subject’ as an identifiable person ‘incorrectly suggests that privacy cannot be violated without identifiability’ (Ibid). This would seem to be an important piece of data protection, yet is absent. Whilst there may be recourse to remedy in other forms of regulation, such as anti-discrimination, this may be hindered by the fact that algorithmic profiling is creating new categories of discrimination which may appear harmless and use categories outside those traditionally recognized in law or utilize ‘proxies’ (such as postcodes), which mask potentially sensitive categories such as ethnicity or income (Mann and Matzner 2019). Mittelstadt highlights legal scholarship concerning groups’ ‘shared ownership of identity’, an area generally ignored by data protection legislation (Mittelstadt 2017, 479).

**Concluding remarks**

The preceding analysis has considered three main problem representations of ‘risk’ in the GDPR, being: (1) the risk to the security of personal data; (2) the risks to people associated with mutable norms such as ‘well-being’ and ‘public interest’; and (3) the risk to the development of the EU’s economy should the ‘free flow’ of data be hindered. The analysis has highlighted the tension between the GDPR’s aims of protecting both the free flow of data and people. We have also highlighted conflicts inherent in balancing public interest framed as economic well-being against privacy rights. The GDPR effectively legitimizes profiling and other forms of surveillance which ‘may impinge on the very essence of our right to privacy’ and have ‘a chilling effect on democracy, creativity and innovation’ (FRA (European Union Agency for Fundamental Rights) 2018, 348). Notwithstanding the fact that the GDPR provides EU residents with a higher level of data protection than elsewhere in the world, the very act of regulating (as opposed to prohibiting) practices such as profiling and algorithmic decision-making in certain circumstances serves to legitimize these practices and does little to negate the power asymmetries of surveillance capitalism. Also legitimized is the amassing of personal information by platform giants and data brokers in the period preceding the GDPR’s enactment. Legal bases such as consent arise in response to a problem representation of individual lack of control, yet fail to provide it due to both the complexity of notice and consent procedures and power discrepancies in the platform economy. Finally, the legal bases for processes such as profiling and automated decision-making do not sufficiently tackle the normative questions around profiling.
A trajectory of data protection discourse which moves away from privacy rights in favor of economic well-being is more likely to produce policy and regulation more accepting of surveillance technologies and practices. To alter this trajectory, a re-conception of privacy is required which is beyond ‘a form of protection for the liberal self’ to more squarely confront economic ‘imperatives’ (Cohen 2013, 1904). Further research is also needed into the anti-democratic effects of surveillance practices such as those engaged in by data brokers, and which continue despite the Regulation’s stated aims of increasing user control and transparency. The view that profiling may proceed if individuals are aware of it should be fully explored as a basis for consent, given that mere awareness does not necessarily negate its potentially discriminatory effects. Until EU regulation confronts the widening power asymmetries of surveillance capitalism, data protection provisions will do little to genuinely protect EU residents from the surveillance practices at the heart of this business model.

**Disclosure statement**

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

**Notes on contributor**

*Michaela Padden* is a PhD student in political science at Karlstad University, Sweden. Her research concerns data protection regulation and its relationship to surveillance technologies tied to platform capitalism, such as profiling and tracking, and their impact on democratic political systems. She has previously worked as a Principal Policy Analyst in the New South Wales Government in Sydney, Australia.

*Andreas Öjehag-Pettersson* is a political scientist at Karlstad University, Sweden. His research interests include the marketisation and privatisation of the public sector and how these concepts relate to knowledge, specifically policy expertise. He is also interested in the effects of public procurement, the use of private consultants, and urban and regional development pertaining to the notion of smart cities.

**ORCID**

Michaela Padden [http://orcid.org/0000-0003-3924-315X](http://orcid.org/0000-0003-3924-315X)

Andreas Öjehag-Pettersson [http://orcid.org/0000-0003-4820-278X](http://orcid.org/0000-0003-4820-278X)

**References**


