Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access

A call to support the governance structure of checks and balances for informational power asymmetries

Mahieu, R.; Ausloos, J.

DOI
10.31228/osf.io/b5dwm

Publication date
2020

Document Version
Final published version

Recognising and Enabling the Collective Dimension of the GDPR and the Right of Access

A call to support the governance structure of checks and balances for informational power asymmetries[1]

René Mahieu

Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel

Jef Ausloos

Institute for Information Law, University of Amsterdam & Centre for IT & IP Law KU Leuven

Summary

The digitisation and datafication of European society necessitate a robust ecology of transparency to enable scrutinising and challenging digital infrastructures that govern our lives. The GDPR – and its transparency provisions in particular – play a vital role in this pursuit. Crucially, in light of the strong informational power asymmetries in the digital society, the effectiveness of GDPR transparency measures will depend on their collective use. This contribution aims to highlight this collective dimension of GDPR access rights, emphasising their potential for social justice (with a rich list of real-life examples in the Annex) and the requirements for rendering them effective. We hope the European Commission takes this contribution as a call to action for creating an enabling environment for collective access rights: empowering all actors in the GDPR's ecology of transparency, and unlocking the full potential of the GDPR in safeguarding a fair digital society.

1 This is a lightly revised version of a report that was initially submitted as feedback to the European Commission's evaluation report on the implementation of the GDPR, as mandated by article 97 of the GDPR. The idea for this document came from a workshop on access request advocacy and research we organised at the University of Amsterdam in December 2019. We would like to thank all participants of that workshop for their valuable input, but also more broadly the growing community of activists, journalists and academics that are active in this area. Ultimately, it is through the actions and initiatives of these people that the ecology of transparency can be realised.

1 An Ecology of Transparency

(1) The introduction of the GDPR has reshaped the EU's data protection landscape. At this moment of evaluation and review, we think it is necessary to emphasise the **importance of the collective approaches enabled by the GDPR's "architecture of empowerment"** and to show the essential role of access rights within this design. Indeed, an environment which enables the collective use of access right is a vital safeguard against informational power asymmetries in an increasingly datafied society. We demonstrate this by showcasing a selection of initiatives relating to the exercise of the right of access by a variety of actors: NGOs, active citizens, journalists, litigators and academics. Against this background we map/investigate the collective attempts to harness the right of access for the public good in order to assess the conditions that contribute to or hinder the effective use of the right. The main conclusion is that this architecture works, supporting a thriving ecology of transparency, only when it is backed up by high levels of compliance and proper enforcement, which are currently lacking.

(2) **EU data protection law has a strong collective dimension.** Indeed, contrary to how it is often represented, data protection law is not solely focused on the individual. While it is true that one of the EC's key objectives when first announcing the data protection reform in 2010 was to "strengthen individual's rights" by "enhancing control over one's own data",[2] the GDPR contains multiple elements that specifically enable the collective use of data subject rights, and the use of these rights with the aim to protect public goods. Thereby the GDPR creates some of the conditions that are needed to support a strong EU culture of data protection which functions as a new system of checks and balances to counter informational power imbalances. As Albrecht points out in *Hands of Our Data,* **the aim of the GDPR is to contribute to a process of collective emancipation**.[3]

(3) **The right of access constitutes a pivotal element in a wider 'architecture of empowerment'** designed to democratise control over the processing of personal data in society. We have argued before that the "access right works best when used collectively and is aimed at empowerment and transparency at a societal level"[4] and that "control over personal data can be particularly powerful when exercised collectively".[5] While data subject rights are conventionally understood

2 European Commission. "COM(2010) 609 Final COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - A Comprehensive Approach on Personal Data Protection in the European Union." Brussels: European Commission, 2010. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0609&from=EN.

3 Albrecht, Jan Philipp. *Hands of Our Data!*, 2015. https://www.janalbrecht.eu/wp-content/uploads/2018/02/JP_Albrecht_hands-off_final_WEB.pdf.

4 Mahieu, René L P, Hadi Asghari, and Michel van Eeten. "Collectively Exercising the Right of Access: Individual Effort, Societal Effect." *Internet Policy Review* 7, no. 3 (2018): 16. https://doi.org/10.14763/2018.3.927.

5 Ausloos, Jef, and Pierre Dewitte. "Shattering One-Way Mirrors – Data Subject Access Rights in Practice." *International Data Privacy Law* 8, no. 1 (February 1, 2018): 4–28. https://doi.org/10.1093/idpl/ipy001.

as individual rights which aim to empower individuals, the collective aspect of these rights has also been present since the emergence of data protection legislation.[6]

(4) **This report presents an overview of the ways in which the right of access is used in a reinvigorated EU culture of data protection**. Max Schrems' access request to Facebook is likely the most famous and often cited example of the use of the right of access by an individual in persuit of a collective interest [see example 1: Schrems v Facebook below]. There is however a broader array of civil society actors which use the right of access in various ways in order to pursue public interest and collective goals, and a fairer digital society more broadly. Privacy International, for example, uses the right in multiple campaigns, including to uncover hidden data ecosystems, and reports that "access rights are an important tool for individuals, journalists, and civil society to investigate, review, and expose how personal data is being processed" [see example 2: Access to assess and contest compliance, p.6; Fix AdTech, p.20].[7]

Example 1: Schrems v Facebook

In 2011 Max Schrems, then a law student, asked Facebook for the data it held about him. He received 1200 pages of data and published this on the website Europe-v-facebook.org.[8] On this website he also shared information about what data Facebook has and how to request it.[9] On the basis of the response to his request he filed 22 complainst at the Irish data protection authority. After 3 years he retracted most claims, citing the refusal to provide a formal decision and lack of procedural rights, and the fact that the costs of litigating against the DPA would have been to high.[10] He concluded that "no normal citizen is able to follow through with such a proceeding". However, Schrems was able to continue with one case, financed through the collection of donations, targeting the transfer of his

6 Many historical examples can be cited. Most notably Stefano Rodotà, the first chairman of the Italian Data Protection Authority, emphasized this aspect of the right of access in his 1973 book Computers and Social Control. Moreover, the famous census case before the German Bundesverfassungsgericht (Federal Constitutional Court) which brought the value of informational self-determination into European legal consciousness was brought by a group of data protection academics. Furthermore, according to Westin the right of access could play an important and necessary role to empower people and counter societal problems such as discrimination. For a more comprehensive analysis of the foundations of data protection see: Mahieu (forthcoming) Exploring the foundations of data protection: A critical history of the right of access to personal data.

7 Privacy International. "A Guide for Policy Engagement on Data Protection -- Part 4: Rights of Data Subjects," August 2018: 53. https://privacyinternational.org/sites/default/files/2018-09/Part%204%20-%20Rights%20of%20Data%20Subjects.pdf.

8 Olivia Solon, 'How Much Data Did Facebook Have on One Man? 1,200 Pages of Data in 57 Categories', Wired UK, 28 December 2012, https://www.wired.co.uk/article/privacy-versus-facebook.

9 'Europe-v-Facebook Data Pool', europe-v-facebook.org, accessed 13 May 2020, http://europe-v-facebook.org/EN/Data_Pool/data_pool.html.

10 'Europe-v-Facebook Complaints', europe-v-facebook.org, accessed 13 May 2020, http://europe-v-facebook.org/EN/Complaints/complaints.html.

personal data outside Europe. In October 2015, this resulted in the Court of Justice of the EU famously invalidating the Safe Harbor rules.[11]

In 2014 Schrems started a new procedure against Facebook in Austria based on the complaints that the Irish DPA had not decided on.[12] The case was started as a class action with the number of participants was limited to 25.000 people, although 60.000 people responded to his call.[13] However, in 2018 The Court of Justice ruled that Schrems could file an individual claim but not a class action.[14] The case is currently still ongoing at the Vienna Regional Court for Civil Matters.[15]

(5) The examples of collective use show that **the role and function of the right of access must be understood in the context of what can be called an "ecology of transparency"**.[16] An ecology of transparency is the intra-institutional network of actors, laws, norms and practices in which the right of access is being exercised. It is shaped by the interplay between the law, the regulators and the actual practices of civil society. Taking this broader view on the ecosystem of institutions and practices allows us to better identify the social conditions that need to be in place for the right of access to achieve its goal of enabling citizens to assess and contest systems that rely on the processing of personal data.

(6) **While the right of access is a fundamental right,** which is in itself central to the protection of other fundamental rights, **there is abundant evidence that compliance with the obligation to respond to access requests is low**. Complaints about access requests not being fulfilled are the most common complaints for data protection authorities. For example, in the last year, almost 40% of the complaints received by the UK ICO were about access requests,[17] and almost 30% of the complaints received by the Dutch DPA were about data subject rights, with a substantial part concerning the right of access.[18] Academic research

11 CJEU Judgement of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650

12 http://www.europe-v-facebook.org/sk/CJEU_en.pdf

13 Ingrid Lunden, 'European Facebook Class Action Suit Attracts 60K Users As It Passes First Court Hurdle', accessed 13 May 2020, https://techcrunch.com/2014/08/21/european-facebook-class-action-suit-attracts-60k-users-as-it-passes-first-court-hurdle/.

14 CJEU Judgement of 25 January 2018, *Maximilian Schrems v Facebook Ireland Limited*, C498/16, ECLI:EU:C:2018:37

15 noyb. (2020, February 26). Facebook witness: 9 ½ hours of "we don't know." Noyb.Eu. https://noyb.eu/en/facebook-witness-9-12-hours-we-dont-know

16 See: Mahieu, René L P, Hadi Asghari, and Michel van Eeten. "Collectively Exercising the Right of Access: Individual Effort, Societal Effect." *Internet Policy Review* 7, no. 3 (2018): 16. https://doi.org/10.14763/2018.3.927. And in the context of the Freedom of Information Act in which the term was originally used: Kreimer, Seth F. "The Freedom of Information Act and the Ecology of Transparency." *Faculty Scholarship* Paper 192 (2008): 1011–80. http://scholarship.law.upenn.edu/faculty_scholarship/192

17 See Information Commissioner's Office. (2019). *Annual Report and Financial Statements 2018-19*, p.32.

18 See Autoriteit Persoonsgegevens. (2020). *Klachtenrapportage 2019*. Retrieved April 1, 2020, from https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/klachtenrapportage_ap_2019.pdf

confirms that non-compliance with access requests is wide-spread.[19] Some issues appear particularly problematic. Notably, the alleged impossibility to verify the identity of the data subject is regularly used by data controllers to stall or block legitimate access requests [see e.g. Fix AdTech, p.20].[20]

(7) This report provides the European Commission – and policy makers (including Data Protection Authorities) more broadly – as well as current and potential users of SARs (journalists, activists, labour unions, etc) with an **overview of the different ways in which the right of access to personal data is used to pursue a variety of collective interests**. For policymakers, it is important to understand how the right of access is functioning in practice within the overall regulatory framework of data protection. Where, following this first review of the GDPR,[21] the tensions and problems indicated in this report can be addressed, the effectiveness of data protection regulation will be greatly improved.

(8) The report is organised as follows. Section 2 shows how various societal actors make use of the right of access in a number of different ways to support the fundamental rights of data protection, as well as other fundamental rights. Section 3 shows that the legal framework of the GDPR is intentionally designed as an "architecture of empowerment", the success of which depends on the activity and mutual support of the various actors. The last section, points out how a lack of compliance and effective enforcement by DPAs risks to subvert the GDPR's empowering potential to counter informational power asymmetries. In light of this, we therefore **strongly recommend the Commission to ensure effective enforcement and recognise the important collective dimension of access rights** (exercised in collectively and/or in pursuit of collective interests). The annex provides a broad selection of collective uses of the right of access.

2 The Right of Access' Goal: Countering Information Asymmetries

(9) In this section we want to point the European Commission's attention to a number of initiatives where the right of access in its collective dimension has been exercised with the overall goal of countering information asymmetries, both in the context of the fundamental rights of privacy and data protection and in the context of other fundamental rights.

19 According to empirical research conducted by the authors a large proportion of organizations do not provide an adequate response to access requests (See Mahieu and others, 2018; Ausloos and Dewitte, 2018).

20 See eg Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 International Data Privacy Law 105; Chris Norval and others, 'RECLAIMING Data: Overcoming App Identification Barriers for Exercising Data Protection Rights', *Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers* (ACM 2018) <http://doi.acm.org/10.1145/3267305.3274153> accessed 28 September 2019.

21 See Article 97 GDPR

2.1) *Safeguarding the Fundamental Right to Privacy (Art.7 Charter) and Data Protection (Art.8 Charter)*

(10) With so many aspects of contemporary society being digitised and datafied, there is a **growing urgency for the ability to scrutinise and contest digital infrastructures or ecosystems**. As illustrated by the many cases in the Annex, GDPR transparency measures – and the right of access in particular – offer a crucial legal tool for investigatory research into data infrastructures, identifying *what* data is collected, *how* and *why* it is processed, with whom it is shared, and so on.

(11) The information that can be obtained through an access request relates to the specific processing of personal data as it relates to one specific person (data subject). Nevertheless, the data obtained through this tool is often used to help understand the ways in which an otherwise opaque organisation processes personal data in general. For example, Privacy International used the right of access to understand the ways personal data is processed by companies in the data broker, ad-tech and credit-referencing industries [see e.g. Example 2, below]. Following their investigations, they filed complaints with three data protection authorities about the alleged unlawful data practices of these companies.

> **Example 2: Access to assess and contest compliance**
>
> Privacy International submitted complaints to the Information Commissioner Office (ICO), (i.e. UK DPA) against seven companies (data brokers, ad-tech companies, and credit referencing agencies).[22] Access requests had a significant role in providing evidence and building the arguments for the alleged breaches of the law by these companies. The complaints show that while responses to access requests are far from complete, they can, in line with GDPRs stated intent, be used to "verify the lawfulness of the processing". In particular, they show that companies are processing data in ways that are not set out in the respective privacy policies.
>
> The case also shows that responses are often inadequate, limiting the potential of the right. Privacy International finds that responses often refer back to privacy policies, and that sources and recipients of data are rarely specifically mentioned. Even when specific sources are mentioned, this information is rarely coupled to specific data. Moreover, when companies engage in profiling and give access to the data that went into the profile, they do not reveal how that data contributed to specific classifications in the profiling. Privacy International applied verious startegies to overcome the limitataions of the responses. For example: they were able to understand the data processing better by comparing responses to access requests from companies that share data between them.

22 Privacy International, 'Our Complaints against Acxiom, Criteo, Equifax, Experian, Oracle, Quantcast, Tapad', accessed 12 May 2020, http://privacyinternational.org/advocacy/2426/our-complaints-against-acxiom-criteo-equifax-experian-oracle-quantcast-tapad.

(12) Various digital rights organisations have also built digital tools that facilitate the exercise of data subject rights. [See example 3, below and other examples in: Tools to facilitate the exercise of data subject rights, p.36]

EXAMPLE 3: TOOLS TO FACILITATE ACCESS

MyDataDoneRight developed by Bits of Freedom, a digital rights organisation in the Netherlands, is an example of a tool to facilitate access requests [see also p.36]. It was launched in 2018 around the time of the introduction of the GDPR. The tool is currently available in three languages – English, French and Dutch – and through partnerships with local NGOs in other member states will be made available across Europe, supporting local languages and including localised contact lists. Bits of Freedom also regularly publishes blog posts about the use of data subject rights and MyDataDoneRight (in Dutch). In these posts various issues are discussed such as which barriers to the effective use of the rights users experience, and whether these are legitimate. Moreover, the platform is used to support other awareness raising campaigns. For example, in 2019 blogger 'JerryHopper' posted about the neighbourhood hub app 'Nextdoor'. In his posts he revealed how to get access to closed neighbourhood groups, and therefore access to the personal data of those people in those groups, by falsifying address data. When a consumer television program reported on this, they invited Bits of Freedom to their show. Bits of Freedom called on people to request their data and ask for removal. Approximately 6000 people did with the help of the MyDataDoneRight tool.

(13) The use of the right of access by **journalists** provides another way in which the right of access can be used to uncover the network of transactions of personal data, **raise awareness** of the public about, and assess the lawfulness of such practices.

EXAMPLE 4: ACCESS FOR INVESTIGATIVE JOURNALISM

In a radio programme about the use of personal data in society (in the context of the introduction of the GDPR), a journalist tried to uncover how it was possible that a cosmetic surgery clinic, of which she had not been a client, nonetheless sent a personalised advertisement to her home address. As a first step, she sent an access request to the clinic, and asked them how and why they had gotten hold of her name and address. The clinic responded that they did not themselves had access to her data, but that their advertisement agency had. The agency had bought contact details of women in a certain age group and living in a certain area from a data broker. Subsequently the journalist filed a request with the data broker and it turned out that they had bought her address from PostNL, the Dutch national postal service. After inquiring with the postal service, she found out that in the small-print of their services to automatically forward mail to a new address after moving house, it was indicated that the company would share this data with third parties for marketing purposes.

(14) The examples above, as well as numerous other examples [e.g. Schrems v Facebook, p.24; Tinder, p.35; and Location-data and smartphone apps, p.33] demonstrate how **targeted access requests, coordinated by activists or journalists can force transparency from the relevant actors and result in better understanding of the underlying data processing ecosystems**. The cases also show that exploring and understanding data infrastructures will often only be the first step, often followed by analysis, evaluation and potential legal action (e.g. examples 1 and 2 above and Fix AdTech, p.20.).

2.2) *Safeguarding Other Fundamental Rights*

(15) Access rights are often used collectively to pursue social justice goals that go beyond data protection and privacy. In light of how they empower individuals to obtain fine-grained information about the data infrastructures that surround and have an impact on them, **access rights can be very valuable in pursuing (social) justice goals**. Information from access rights may be used to seek inferences, data and meta-data about prediction and training data which can reveal how systems function and affect individuals/society.[23] This information may be compiled to shine light on the functioning of a model,[24] or compared across individuals, demographics or applications so as to reveal potential discriminatory practices. Access rights might also be able to shine light on where models come from, which actors were involved in training and building them, and when. This can be important in a wide variety of circumstances, not in the least to lay bare and scrutinise the 'manipulative potential of algorithmic processes', the importance of which has recently been confirmed by the Council of Europe.[25] The OpenSchufa, p.26; Uber, p.29 and FairTube, p.29 cases provide evident illustrations of how crowd-sourcing access rights can be used to achieve social justice aims.

EXAMPLE 5: ACCESS FOR FAIRNESS IN THE PLATFORM ECONOMY

The so-called platform/gig economy has a massive impact on labour rights and social justice more broadly.[26] Access rights are used by various labour rights movements, in particular in the platform economy. One

23 Jef Ausloos and Michael Veale, 'Researching Through Data Rights' [2020] Forthcoming.

24 Some work has recently shown that model reconstruction attacks can be heightened by the use of model explanations. See eg Smitha Milli and others, 'Model Reconstruction from Model Explanations', *Proceedings of the Conference on Fairness, Accountability, and Transparency* (ACM 2019) <http://doi.acm.org/10.1145/3287560.3287562> accessed 24 June 2019. Work is ongoing to understand what explanations can be used to reveal about models, see further Martin Strobel, 'Aspects of Transparency in Machine Learning', *Proceedings of the 18th International Conference on Autonomous Agents and MultiAgent Systems* (International Foundation for Autonomous Agents and Multiagent Systems 2019) <http://dl.acm.org/citation.cfm?id=3306127.3332143> accessed 24 June 2019.

25 Council of Europe, Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes 2019 [Decl(13/02/2019)1]. This declaration stresses the societal role of particularly academia, 'in producing independent, evidence-baed and interdisciplinary research and advice for decision-makers regarding the capacity of algorithmic tools to enhance or interfere with the cognitive sovereignty of individuals'.

26 https://privacyinternational.org/case-study/751/case-study-gig-economy-and-exploitation

example is labour union Worker Info Exchange, which uses the right of access for Uber drivers to get access to the data that Uber holds on them [see also, p.29].[27] Drivers currently do not have access to basic data such as their log-off/on times to the platform (necessary in order to calculate the effective hourly income). Getting access to their data is a way to balance the information-driven power asymmetry between drivers and the company. Eventually this could support their fight for fundamental labour rights such as a minimum wage.

EXAMPLE 6: ACCESS FOR ALGORITHMIC ACCOUNTABILITY

Another paradigmatic example of the use of access rights for social justice is the campaign by NGOs Algorithm Watch and Open Knowledge Foundation Deutschland called "OpenSCHUFA" [see also p.26].[28] This was a campaign based on access requests to create and demand transparency on the functioning of Schufa's credit scoring algorithm. Schufa is the largest credit scoring agency in Germany. Its scores are used to determine if people can get a loan, a telephone contract and rent an apartment. Civil society organisations have long demanded that there should be transparency about how this score is calculated. Citizens have individually used the right of access to gain insight into their score, and on how their score was calculated. In response to access requests, Schufa provided access to the personal data that was used to calculate the score, as well as to the score itself. In 2014 the Bundesgerichtshof (German supreme court) in a case against Schufa decided that the individual did not have a right to know the weight that specific elements have in the determination of the final credit score, nor information on comparison groups. For the OPENSchufa project 4,000 people shared the response of their access requesta with the NGOs. Based on the personal data and credit scores contained in those responses they were able to partly reverse engineer the scoring algorithm.

(16) Moreover, access rights are also **becoming increasingly relevant as part of evidence seeking in cases** where the dispute is not fundamentally about the lawfulness of the processing of the personal data as such. (e.g. disputes related to issues of criminal,[29] employment,[30] financial,[31] fiscal,[32] immigration,[33] trust[34] or

27 https://www.opensocietyfoundations.org/voices/q-and-a-fighting-for-workers-right-to-data; https://www.economist.com/britain/2019/03/20/uber-drivers- demand-their-data

28 https://openschufa.de/english/

29 *Kololo v Commissioner of Police for the Metropolis* [2015] EWHC 600 (QB). *Lin & Anor v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB).

30 E.g. *Ittihadieh v 5-11 Cheyne Gardens RTM Company Ltd & Ors* [2017] EWCA Civ 121.

31 E.g. *X v Dexia Bank Nederland NV* [9 maart 2005] Rechtbank Zwolle-Lelystad 103434 / HA RK 04–215, ECLI:NL:RBZLY:2005:AS9407; *X v Y* [2018] ECLI:NL:PHR:2018:1273 (Parket bij de Hoge Raad).

32 E.g. Amélie Lachapelle and Elise Degrave, 'Le Droit d'accès Du Contribuable à Ses Données à Caractère Personnel et La Lutte Contre La Fraude Fiscale, Revue Générale Du Contentieux Fiscal, 2014, 5, p. 322-335'.

defamation proceedings.[35]) Many of these cases are **about the resolution of structural injustices** that often involve large groups of people. The goal can be both to create change for the individual involved in the case, as well as (deliberately or not) creating societal change.

EXAMPLE 7: access to seek evidence

An example of this type of cases is the use of the right of access to personal data in the *Dexia* cases in The Netherlands.[36] To understand the relevance of this case it is important to know that one particular aspect of the Dutch financial landscape before the financial crises of 2008 was that, spurred by specific fiscal rules, financial institutions had started to sell complex and risky products to the general public. A popular consumer protection television programme, *Radar*, advised clients of banks who had bought such products to file access requests to acquire data that could help prove the wrongdoing by the banks in court, and provided the template for such request. Against this background, thousands of clients used their right of access to request data from Dexia, one of the banks that had sold these financial products. The clients requested their complete file including in particular a copy of the contracts between the clients and the bank, their risk profile and a transcription of recordings the bank made of telephone conversations it had with the clients. While the bank initially denied access to the files the Dutch Supreme Court eventually decided that access had to be provided. The files obtained through the access requests were later used in class action lawsuits against the financial institutions.

3 The GDPR: A Legal Framework Empowering Society

(17) The GDPR explicitly acknowledges the role of various actors in the governance of data protection. Rather than relying primarily on a top down "command and control" type of regulation which is based on control by a central regulatory body,[37] **the GDPR explicitly enables citizens and civil society to participate in checking the compliance of data controllers with the Regulation**. Therefore, the development of collective practices, as described in the previous section and the Annex, should be understood as a process of societal appropriation of the legal toolkit which is a direct expression of the intended design of the GDPR.

(18) According to Recital 63 GDPR, "A **data subject** should have the right of access to personal data which have been collected concerning him or her, and to exercise

33 E.g. Joined Cases C-141/12 and C-372/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* ECLI:EU:C:2014:2081.

34 E.g. *Dawson-Damer & Ors v Taylor Wessing LLP* [2017] EWCA Civ 74.

35 E.g. *Rudd v Bridle & Anor* [2019] EWHC 893 (QB).

36 Dexia [2007] ECLI:NL:HR:2007:AZ4664.

37 Baldwin, Robert, Martin Cave, and Martin Lodge. *Understanding Regulation: Theory, Strategy, and Practice*. 2nd ed. New York: Oxford University Press, 2012: 106-111.

that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing." In this light, the discourse of 'empowering data subjects' should be understood as going beyond their mere ability to control which data is held by whom and to make decisions about the limits of data sharing by indicating "privacy preferences" through privacy dashboards and cookie banners, correcting incorrect information, or porting data to another service provider.

(19) The role of **civil society** in data protection has been specifically strengthened by the introduction of the GDPR. In particular, article 80(1) GDPR provides a specific role for not-for-profit organisations by affording them the right to make complaints and litigate in the name of data subjects. In some member states, NGOs are also entitled to file complaints independently of data subject's mandate.

(20) The primary task of the **Data Protection Authority** (DPA) is to monitor and enforce the GDPR. This includes handling complaints by data subjects or civil society organization (article 57(f) GDPR). Contrary to the situation under the DPD, DPAs are obliged to handle all complaints.[38]

(21) The **Data Protection Officer** (DPO) is another important actor in the governance structure of the GDPR. According to Article 39(1)(b) GDPR, one of the tasks of the data protection officer is to monitor whether the data controller is compliant with the law. The provisions in article 38 are intended to ensure that DPOs are independent in their task and have a direct line with the highest level of management of the controller. They are also directly related to DPAs and data subjects. When data subjects have questions or complaints about the processing of data by the data controller, they can contact the DPO. The DPO also serves as contact point with the DPA.

(22) Next to these functions which are explicitly acknowledged in the GDPR, the "ecology of transparency" also crucially includes other actors in society. A particularly important role in data protection is played by the **media and academia**. The role of the media consists in providing fundamental checks and balances in a free democratic society and its freedom is protected as a fundamental right in Europe under article 11(2) of the Charter. An active civil society and media are important aspects of democratic societies as they are elements of a system of balance of power. They help bring attention to the most pressing societal problems. In this role, they help guide the limited resources of formal enforcement bodies in the right direction.

(23) **All actors within the "ecology of transparency" are dependent on each other in various ways**. It is clear that data subjects depend on support by civil society

38 Because resources are severely restricted, the depth of the investigation is in many cases limited. Moreover, in some member states this has led to a situation where because of a backlog, complaints are only picked up after half a year (see e.g. https://www.rtlz.nl/tech/artikel/5020511/autoriteit-persoonsgegevens-tekort-drukte-privacyklachten-avg-d66-sp). The chairman of the Dutch DPA warns that "In essence, you say: we protect your privacy well through legislation. However if the supervisor does not have sufficient resources, you make it a non-existent right. Because we cannot enforce it sufficiently"" [Dutch original: "Feitelijk zeg je: we beschermen je privacy goed via wetgeving. Maar als de toezichthouder niet over voldoende middelen beschikt, maak je het een niet bestaand recht. Want we kunnen niet voldoende handhaven"].

organisations, as these organisations provide various kind of support. For instance, they provide tools that facilitate data subjects in exercising their data subject rights, including advice and legal support when data subjects have questions about data protection law or complaints about data controllers. Similarly, data subjects are dependent on the strength and position of the DPO and DPA, as a strong and independent DPO and DPA can play an important role in guiding organizations towards compliance with data subject rights. Conversely, when the position of the DPO and DPA is weak, data subjects have less chance to rely on them to ensure compliance with their rights.

(24) While the GDPR provides an "architecture of empowerment" that aims to resolve informational power asymmetries, a closer look at many of the practical examples (cf. Annex) demonstrates that their success is often achieved despite serious shortcomings in compliance. The effectiveness of the right of access in particular is impeded by the fact that requests are often ignored and many responses to access requests are incomplete. Alternative strategies are frequently used to overcome shortcomings of access requests (elsewhere, we have described ways to overcome data controller strategies to illegitimately block data rights)[39]. For example, journalists often find that they get access to requested information only after they reveal to the controllers that they are journalists [e.g. Facebook contact import, p.32; Tinder, p.35]. Moreover, the limited information acquired through access requests most of the time provides little insight and needs to be complemented with other sources of information from privacy policies, as well as companies publicly available business-to-business marketing materials, patent filings, or through technical observation [e.g. Tinder, p.35] In many other cases, complex and expensive legal actions are required to force controllers to comply with legitimate requests.

(25) One of the aims of the GDPR is to give people control over their data. Yet, while the GDPR was heralded for putting in place an architecture for empowerment over data, a large and **growing proportion of people feel that they do not have control over information they provide online**.[40] This is arguably a consequence of the lack of compliance and enforcement of data subject rights.[41] Providing rights and raising awareness about these rights without ensuring compliance through enforcement, may in fact be contributing to a growing awareness of loss of control. When left unabated, these problems may result not only in effective disempowerment of data subjects, but potentially also in disappointments and defeatism as to the ability of data protection rules to effectively protect

39 Ausloos, Jef, Réne Mahieu, and Michael Veale. 'Getting Data Subject Rights Right A Submission to the European Data Protection Board from International Data Rights Academics, to Inform Regulatory Guidance'. *Jipitec* 10, no. 3 (21 February 2020). https://osf.io/e2thg.

40 See notably: Eurobarometer 2019. (2019). European Commission; Strycharz, Ausloos & Helberger (2020), Data Protection or Data Frustration? Individual perceptions and attitudes towards the GDPR. (Forthcoming)

41 As evidenced in Ausloos, Jef, and Pierre Dewitte. 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice'. *International Data Privacy Law* 8, no. 1 (2018): 4; Mahieu, René L. P., Hadi Asghari, and Michel van Eeten. 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect'. *Internet Policy Review* 7, no. 3 (13 July 2018). https://policyreview.info/articles/analysis/collectively-exercising-right-access-individual-effort-societal-effect.

individuals.[42] Moreover, **these issues undermine the GDPR's "architecture of empowerment",** the well-functioning of which is a precondition for higher levels of compliance and generating trust in the data society.

4 Recommendation: Empowering Citizens by Promoting the GDPR's Collective Dimension and Strengthening Enforcement

(26) The effectiveness of the 'ecology of transparency' depends on the effectiveness of its individual components, i.e. the network of actors, laws, norms and practices in which the right of access is being exercised – and their ability to mutually reinforce each other. **Active citizens, digital rights organisations, the media and academia interact with each other and function together as a network of checks and balances vis-a-vis other powers in our society**.

(27) Because of their severity in the current digital society, major information and power asymmetries cannot be addressed effectively by data subjects acting alone. It is in recognition of this reality that the GDPR provides a broader architecture of empowerment. Yet the importance of the collective dimensions underlying the GDPR – and resulting from it – has not been properly recognised. **When applying the GDPR, or considering any modification of the Regulation, the competent institutions – the European Commission, the EDPB, the DPAs and the EDPS – should take into consideration, value and strengthen these collective elements, as they are crucial in enabling a full realisation of the potential of the GDPR.**

(28) In light of the increased 'datafication' of society, the right of access to personal data is one of the most important tools in its toolbox. In fact, civil society actors say that access requests are essential to the work they are doing on a daily basis.[43] However, the effectiveness of this tool depends to a large extent on the willingness of data controllers to provide the requested information. Clearly, the commitment to take seriously their obligation to respond to access requests is dependent on the expected risk of enforcement in case of non-compliance. In other words, **the strength of the right of access as a tool to scrutinise and challenge data infrastructures governing our lives, crucially depends on adequate enforcement by DPAs and courts**.

(29) **Data controllers structurally fail to fully comply with access requests**, as is demonstrated by various empirical studies and many of the cases in the Annex. In those cases, data subjects will often have to rely on data protection authorities to make sure the GDPR transparency requirements are effectively and adequately complied with by data controllers. Despite the fact that DPAs are explicitly tasked

42 Andrew Hilts and Christopher Parsons, 'Access My Info: An Application That Helps People Create Legal Requests for Their Personal Information', *Data Privacy Tools* (2015).

43 See for example: panel on access requests as a tool for activism, Privacy Camp 2020. https://www.youtube.com/watch?v=m60l0C8rojE&list=PLGeR6jS_7N7f_msH4BN-WT64roFWAXfj2&index=7&t=0s

to monitor and enforce the application of the GDPR (cf. Art.57 GDPR), and have extensive powers to do so, in practice their enforcement remains relatively weak. **Even where NGOs or academics have filed well-argued and documented complaints for non-compliance with access requests, DPAs have only taken action** occasionally, and if so, very mild [e.g. Fix AdTech, p.20; Right of Access Compliance: Streaming services, p.23]. Civil society organisations have indicated **that the strength of access rights as a tool for holding data processing activities to account is inhibited by the lack of enforcement by DPAs**.[44] Moreover, and significantly, even DPOs have indicated that a lack of enforcement diminishes their ability to guide companies towards more compliant behaviour.[45] Without the added weight of potential financial repercussions (i.e. fines), their voice rings less powerful in the boardroom, where in the end the financial bottom line is the central indicator that guides corporate decision making. In order to reverse this situation, and give any practical use to data subject rights, enforcement needs to be strengthened considerably. In short, the expectation is that when enforcement on the right of access is strengthened in specific cases this will not only have an effect on those cases but will have a ripple effect, by empowering other actors within the ecology of transparency.[46]

(30) Whereas one of the central aims of introducing the GDPR was installing a harmonised and high level of enforcement, this has not yet been realised in practice. In particular, four issues need to be addressed with respect to this lack of enforcement. First, there are quite substantial differences in the level of enforcement between different member-states. Second, the enforcement of access rights does not have priority. Third, enforcement is often slow. Fourth, enforcement is done in multiple steps, inviting data controllers to adopt a wait and see approach. These four issues are addressed below.

(31) **A. Lack of consistency in enforcement across member-states**. The EU is in a unique position to introduce and enforce legislation to increase both the welfare and well-being of its citizens. And, in many cases, EU regulation will also positively effect citizens outside of Europe.[47] However, the decentralised nature of enforcement, through authorities acting at the national level, risks seriously impeding the effectiveness of European regulation.[48] In this respect, the development of the application of chapter 7 of the GDPR (on cooperation and consistency of the supervisory authorities) is going to play a crucial role. The effective functioning of the ecology of transparency will only be possible if this

44 See for example: panel on access requests as a tool for activism, Privacy Camp 2020. https://www.youtube.com/watch?v=m60l0C8rojE&list=PLGeR6jS_7N7f_msH4BN-WT64roFWAXfj2&index=7&t=0s

45 *Report roundtable data protection in the media sector*. (2019). Chair data protection on the ground. https://smit.vub.ac.be/wp-content/uploads/2019/05/Report-roundtable-data-protection-in-the-media-sector_def.pdf

46 See also in the US context for a description of such an effect of increased enforcement by the FTC: Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (1 edition). The MIT Press. pp.194-195.

47 Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review*, *107*(1).

48 Giurgiu, A., Boulet, G., & De Hert, P. (2015). EU's One-Stop-Shop Mechanism: Thinking Transnational. *Privacy Laws & Business*, 16–18.

mechanism will ensure a consistent and high level of enforcement throughout the Union. Currently, the one-stop-shop mechanism risks to seriously impede the right of data subjects to an effective remedy. **The Commission should prioritise a high level of protection of fundamental rights, when assessing the one-stop-shop mechanism.**

(32) **B. There are strong indications that enforcement of access rights is not seen as a priority by DPAs.** The explicit argument for assigning a low priority for enforcing access rights is that the benefits of access are perceived to be restricted to the individual data subject.[49] However, as we have shown in this report (see notably the Annex), compliance with access rights is also vital from a collective and societal perspective. Therefore, we recommend that, **because of their collective relevance enabling the promotion of social justice in a datafied society, access rights should be given high priority in enforcement**.

(33) **C. Enforcement under GDPR is often slow.** Reasons cited for slow enforcement include that many of the questions DPAs are presented with are complex, they are generally underfunded, and lack the technical know-how or capacity to adequately fulfil their tasks pursuant to Art.57 GDPR. **The Commission should insist that member states allocate sufficient funding to DPAs and put in place the necessary mechanisms to hold DPAs themselves accountable to their regulatory targets (e.g. through regular audits and setting minimum enforcement requirements)**

(34) **D.** Prior to the entry into force of the GDPR, many DPAs had very limited enforcement tools at their disposal. In the Netherlands, for example, the DPA did not have the option to impose a fine directly. The most severe option at its disposal was the imposition of a burden under penalty. As Jacob Kohnstam, the former chairman of the Dutch DPA remarked, this resulted in organisations waiting until the regulator knocked on their door and then admit only what was strictly necessary.[50] When, instead, organisations know or expect to get a fine directly when an infringement of the law has been established by the authorities, they have more incentive to comply with their obligations. In order to amend this problem, the GDPR provides the legal basis for direct enforcement in cases of evident non-compliance with the law. In order to reverse the incentive structure, **in case of blatant non-compliance with the law, DPAs should make direct use of the ability to impose administrative fines more often, without first having recourse to other measures.**

---

49 See for example Dekker. (2020, March 23). *Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden* [Letter to Tweede Kamer]. In which the Dutch minister of legal protection responds to parliament that in a situation of restricted capacity at the Dutch DPA complaints about non response to access requests are not prioritised. Another specific example is a 2015 response to a requesst for mediation about non-complaince to an access-request the Dutch DPA explained it strives to the greatest possible radiating effect of the deployment of its capacity, so that as many people as possible are helped or benefit from it, and therefore would not mediate in an individual access request case. See: http://user.math.uzh.ch/dehaye/uber-data-request.pdf

50 Heilbron, B., & Koopman, E. (2019, January 16). De Autoriteit Persoonsgegevens is altijd klein en tandeloos gehouden. De Groene Amsterdammer. https://www.groene.nl/artikel/de-tragedie-van-het-privacytoezicht

(35) We recognise that limited enforcement can partly be explained by the limited resources, especially considering the vast expanse of operations that require investigation and possibly enforce. Indeed, everything in society is datafied in one way or another, which (a) makes those ecosystems incredibly complex to understand; and (b) renders DPAs scope of enforcement infinitely big. **Creating an enabling environment for collective access rights – empowering all actors in the GDPR's ecology of transparency – helps DPAs in dealing with these challenges and effectively achieving the GDPR's regulatory aims**.

5 Conclusion

(36) The GDPR is a progressive piece of legislation. Beyond promoting economic goals, and the protection of fundamental rights, it envisions an active and emancipated citizenry. It invites citizens, and civil society more broadly to participate in the system of checks and balances, providing them the legal tools to do so. The emergent ecology of transparency is becoming an essential and inherent part of a European culture of data protection. As one of the GDPR's centrepieces, **the right of access plays a vital role in enabling scrutinising and challenging emergent data ecosystems governing our society**. Indeed, the right of access is not just essential for enabling data subjects to exercise other GDPR rights and verify compliance with GDPR obligations. Its value extends beyond the individual, and plays a pivotal role in collective efforts to overcome information asymmetries.

(37) The Commission should explicitly and strongly acknowledge the collective value of data subject rights for safeguarding social justice and fundamental rights and freedoms in a datafied society. The enforcement of access rights should therefore be central to the strategies of DPAs.

Annex – Collective Uses of Data Access Rights

A non-exhaustive list

1 Safeguarding data protection and privacy

1.1. Corporate surveillance of climate activists

- *Location*: UK
- *Time*: 2010-2014
- *One-liner*: (climate) activists submit subject access request to get information about corporate surveillance
- *Driving force*: civil society
- *Goal*: receiving information about BP's surveillance of activists
- *Est. number of participants*: unknown

Climate activists were protesting BP on various occasions.[51] After suspicion rose that they were being monitored, individual activists subsequently requested the company what information they held about them. They received the files BP held on them. This information showed how the companies were keeping personal records on them, including their pictures, online activities and presence at protests. Illustrating the monitoring, the results have been documented in academic articles.[52] One of the activists also wrote about the information she received herself.[53]

1.2. Data retention act protested

- *Location*: Germany
- *Time*: 2009-2011
- *One-liner*: infographic shows how much information is held based on data retention laws
- *Driving force*: politicians, journalism (Die Grüne, Malte Spitz)
- *Goal*: informing and mobilising the public in relation to data retention laws, illustrating the invasiveness of the information that is stored
- *Est. number of participants*:-

After the Data Retention Directive was implemented into German Law, the political party "Die Grüne" wanted to campaign against it.[54] The political party started a website which helped people to submit their request by offering templates and information. It called upon the public to file the requests.[55] Malte Spitz, politician for Die Grüne, requested his data from

51 See for instance: 'How We Reclaimed the Bard from BP', 11 January 2013, https://bp-or-not-bp.org/2013/01/11/how-we-reclaimed-the-bard-from-bp/.

52 Julie Uldam, 'Social Media Visibility: Challenges to Activism':, Media, Culture & Society, 21 April 2017, https://doi.org/10.1177/0163443717704997 ; Hans Krause Hansen and Julie Uldam, 'Corporate Social Responsibility, Corporate Surveillance and Neutralizing Corporate Resistance', The Routledge International Handbook of the Crimes of the Powerful, 2015, 186–196.

53 Jess Worth, 'Spied on by BP', New Internationalist, 1 November 2014, https://newint.org/features/2014/11/01/my-spy.

54 Data Retention Directive (Directive 2006/24/EC)

55 Stefan Krempl, 'Grüne starten Auskunftskampagne zur Vorratsdatenspeicherung', Heise Online, accessed 13 May 2020, https://www.heise.de/newsticker/meldung/Gruene-starten-Auskunftskampagne-zur-Vorratsdatenspeicherung-752501.html.

his telecom provider too.[56] Malte Spitz and his telecom provider reached a settlement in which he obtained part of the information the company held on him.[57] He subsequently worked together with newspaper Die Zeit to visualize exactly what his file contained.[58] The infographic shows 6 months of data, revealing his exact whereabouts. The infographic shows how much can be deduced from meta-data and helps support the case against data retention legislation.

1.3. Facebook's 'download your data' tool incomplete

- *Location*: US
- *Time*: 2018
- *One-liner*: US Congressman requests his Facebook data and uses this to check Zuckerberg's responses during Congress hearing
- *Driving force*: US Congressman (Jerry McNerny)
- *Goal*: receiving information for the US House committee
- *Est. number of participants*: 1

In April 2018 the Energy and Commerce Committee of the United States House of Representatives held a hearing of Mark Zuckerberg as the CEO of Facebook.[59] In this hearing the Californian representative Jerry McNerny asked whether users can download all the information Facebook has about them. He said his staff had downloaded the data on the platform and concluded that not all information was included.[60] Zuckerberg stated that all information can be downloaded with the download your data tool. McNerny responded by saying that the data he downloaded did not include browsing history. When McNerny pushes on, Zuckerberg persists that all information is included. After a break, Zuckerberg corrected the answer he had given and clarified that weblogs are not part of the data in the download your data tool.[61]

1.4. Fix AdTech

- *Location*: Europe
- *Time*: 2018-ongoing

---

56 Kai Biermann, 'Vorratsdaten: Grüne wollen Schweigen der Telekom brechen', Die Zeit, 25 August 2009, sec. Digital, https://www.zeit.de/online/2009/35/vorratsdaten-spitz-telekom?page=1

57 Malte Spitz, 'Six months of my life in 35,000 records', Malte-Spitz.de, accessed 13 May 2020, https://www.malte-spitz.de/2011/03/04/six-months-of-my-life-in-35000-records/.

58 'Tell-all telephone', Die Zeit Online, accessed 13 May 2020, https://www.zeit.de/datenschutz/malte-spitz-data-retention.

59 United States Congress House Committee on Energy and Commerce, 'Facebook: Transparency and Use of Consumer Data : Hearing before the Committee on Energy and Commerce, House of Representatives, One Hundred Fifteenth Congress, Second Session, April 11, 2018.' (U.S. Government Publishing Office, 2018), https://purl.fdlp.gov/GPO/gpo109637.

60 Natasha Lomas, 'Zuckerberg Won't Give a Straight Answer on Data Downloads', TechCrunch, 11 April 2018, https://social.techcrunch.com/2018/04/11/zuckerberg-wont-give-a-straight-answer-on-data-downloads/.

61 Amanda Zantal-Wiener, 'New Questions for Mark Zuckerberg Emerge at House Energy and Commerce Hearing', Hubspot, accessed 13 May 2020, https://blog.hubspot.com/news-trends/new-questions-for-mark-zuckerberg-emerge-at-house-energy-and-commerce-hearing.

- *One-liner*: civil society strategically using access rights in investigating the advertisement ecosystem
- *Driving force*: civil society (Panoptykon)
- *Goal*: understanding the real-time-bidding advertisement ecosystem

Panoptykon participated in the "Fix Adtech" complaints against Google and IAB Europe (initiated by Johnny Ryan @ Brave) over the claim that online behavioral advertising in its current form is irreconcilable with the fundamental principles of the GDPR.[62] Panoptykon did its own investigation of the online behavioral advertising ecosystem in Poland, amongst other things by sending access requests to various companies involved in the AdTech ecosystem.[63] They found that in most cases companies refused to provide personal data to users based on alleged difficulty with their identification.[64] They used the responses to these requests to support the argument made in the complaint that the system is not transparent.

1.5. Netflix' Bandersnatch

- *Location*: UK
- *Time*: 2019
- *One-liner*: subject access request to reveal how much information Netflix stores about the choices people make when watching interactive content
- *Driving force*: civil society (Michael Veale)
- *Goal*: revealing how much data Netflix stores based on *Bandersnatch* viewing data , assessing GDPR compliance, and inspiring people to ask for their data
- *Est. number of participants*: 1

In December 2019 Netflix revealed an interactive episode of its film series Black Mirror called Bandersnatch. It is an interactive choose-your-own-adventure film, in which each individual viewer has to make choices for the lead character to at certain points in the episode, thereby influencing how the story will progress.[65] After its release it was suggested that Netflix' main interest would be to gather more data about its users.[66] UCL's Digital Rights lecturer Michael Veale requested Netflix to send him a copy of his data to reveal what

62 Similar complaints have been filed with the data protection authorities in Ireland, UK, Belgium Netherlands, Spain and Luxembourg. Johnny Ryan, 'Ad Tech GDPR Complaint Is Extended to Four More European Regulators', Brave Browser, 20 May 2019, https://brave.com/rtb-complaint-5-new-countries/.

63 Panoptykon, 'Panoptykon Files Complaints against Google and IAB Europe', accessed 12 May 2020, https://en.panoptykon.org/complaints-Google-IAB.

64 *id.* ("This argument - made by key players in the OBA ecosystem - confirms that it has been designed to be obscure. Key identifiers used by data brokers to single out users and target ads are not revealed to data subjects that are concerned. It is a "catch 22" situation that cannot be reconciled with GDPR requirements (in particular the principle of transparency).").

65 Lucas Shaw, 'Netflix Is Planning Choose-Your-Own-Adventure "Black Mirror"', Bloomberg, accessed 13 May 2020, https://www.bloomberg.com/news/articles/2018-10-01/netflix-is-said-to-plan-choose-your-own-adventure-black-mirror; David Streitfeld, 'Netflix Takes Interactive Storytelling to the next Level with "Black Mirror: Bandersnatch"', Independent, accessed 13 May 2020, https://content.jwplatform.com/previews/ssFVPSEd-9ygSIn9G

66 See for instance: Viridiana Romero Martinez, 'Black Mirror Bandersnatch: Data Mining Your Decisions', Medium, accessed 13 May 2020, https://medium.com/datadriveninvestor/black-mirror-bandersnatch-data-mining-your-decisions-afad5ea71158; and Jesse Damiani, 'Black Mirror: Bandersnatch Is Netflix's Trojan Horse to Profit', The Verge, accessed 13 May 2020, https://www.theverge.com/2019/1/2/18165182/black-mirror-bandersnatch-netflix-interactive-strategy-marketing.

data Netflix stored about the choices he had made while watching Bandersnatch. He published the data he received from Netflix and commented on them.[67] He found that Netflix did store information about the choices people made even after they had watched the film linked to their accounts. The data Netflix provided reveals the choices Michael Veale made, whether he has seen the segments before and the platform he used. Netflix claimed the legal basis for the processing is that the processing is necessary for the performance of a contract. Netflix did not provide information on how long they stored the information. Michael Veale also noted that it's possible that Netflix complied with his request because he is a public figure.[68]

1.6. Right of Access Compliance: Marktplaats

- *Location*: Netherlands
- *Time*: 2012-2014
- *One-liner*: journalist requests his personal data and received data on others as well
- *Driving force*: journalism, civil society
- *Goal*: revealing a problem with the handling of personal information by auctioning website
- *Est. number of participants*: 3

Marktplaats is a Dutch classified advertising website, allowing people to put up their own adverts. In 2012 activist Rejo Zenger asked Martkplaats for his personal information and received far more than that. The file contained IP-addresses, telephone numbers, email addresses and location details of the people that posted the adds he responded to. He publishes this on his blog.[69] Two years later, Douwe Schmit requested his own data at Martkplaats and experienced the same thing. He wrote about his finding in an article on the online news website De Correspondent.[70] The journalist explains how this is a violation of Martkplaats's own terms, but also data protection law. The article further shows that this is not an exception, mentioning Rejo Zenger's earlier article and adding how Sammy Hemerik received third person information when she asked for her data as part of her graduation project. The article explains and illustrates why this is problematic.

1.7. Right of Access Compliance: Social media companies

- *Location*: Germany
- *Time*: 2018

---

67 Michael Veale, 'Netflix Claim They Only Use Individual Choices to Inform Which Video Segments to Show, Although They Do Learn from Aggregate Choices, as Would Be Expected.', Twitter, accessed 13 May 2020, https://twitter.com/mikarv/status/1095110950028562433.

68Matthew Gault, 'Netflix Has Saved Every Choice You've Ever Made in "Black Mirror: Bandersnatch''"', Vice, accessed 13 May 2020, https://www.vice.com/en_us/article/j57gkk/netflix-has-saved-every-choice-youve-ever-made-in-black-mirror-bandersnatch.

69 Rejo Zenger, 'Marktplaats.nl geeft inzage in andersmans gegevens', Rejo Zenger's blog, accessed 12 May 2020, https://2019.rejo.zenger.nl/focus/marktplaats-nl-geeft-inzage-andersmans-gegevens/.

70 Douwe Schmidt, 'Gratis af te halen bij Marktplaats: persoonsgegevens van derden', De Correspondent, accessed 13 May 2020, https://decorrespondent.nl/1251/gratis-af-te-halen-bij-marktplaats-persoonsgegevens-van-derden/48601292454-afe96caa.

- *One-liner*: consumer organization researches how social media companies respond to subject access requests
- *Driving force*: civil society
- *Goal*: verifying whether social media companies are compliant with regard to GDPR access requests
- *Est. number of participants*: unknown

The German consumer association of North Rhine Westphalia wanted to know to what extend social media companies are compliant with the – then newly introduced – GPDR.[71] Its 'Market watch team' conducted its research by reading privacy policies of eight companies and additionally send subject access requests.[72] The companies were: Facebook, Instagram, LinkedIn, Pinterest, Snapchat, Twitter, WhatsApp, YouTube/Google. The Market watch teams also looked at data download tools. It finds that none of the companies were fully compliant.[73] Although all companies responded within the required six weeks, the responses lacked information, were written in English (while the request was in German), or referring to the data download tools. Regarding the data download tools it finds that they do not provide users with all the information they are entitled to.[74]

1.8. Right of Access Compliance: Streaming services

- *Location*: the Netherlands, UK, Ireland, Luxembourg, Austria, Sweden and Germany (Berlin)
- *Time*: 2018-2019
- *One-liner*: investigate what data streaming services collect
- *Driving force*: civil society (NOYB)
- *Goal*: testing compliance with GDPR access requests

NOYB sent access requests to eight streaming services in eight different member states.[75] In January 2019 NOYB filed complaints with data protection authorities for several violations of the requirements of Article 15 GDPR. While complaints about the services vary depending on the differences in the responses given, some elements are present in most of the complaints. According to NOYB the responses do not comply with the GDPR for several

71 Marktwächter Digitale Welt, 'Soziale Medien und die DSGVO', Die Marktwächter, accessed 13 May 2020, https://www.marktwaechter.de/digitale-welt/marktbeobachtung/soziale-medien-und-die-dsgvo.

72 The full reports in German can be found here: Marktwächter Digitale Welt, 'Soziale Medien Un Die EU-Datenschutzgrundverordnung - Teil I' (Verbraucherszentrale NRW, September 2018), https://www.marktwaechter.de/sites/default/files/downloads/bericht_soziale_medien_dsgvo_i.pdf; Marktwächter Digitale Welt, 'Soziale Medien Un Die EU-Datenschutzgrundverordnung - Teil II' (Verbraucherszentrale NRW, December 2018), https://www.marktwaechter.de/sites/default/files/downloads/bericht_soziale_medien_dsgvo_ii.pdf; A press release in English can be found here: Marktwächter Digitale Welt, 'Social Media and the GDPR: Consumers Should Expect Better', Marktwächter, accessed 13 May 2020, https://www.marktwaechter.de/sites/default/files/downloads/social_media_and_the_gdpr.pdf.

73 Marktwächter Digitale Welt, 'Soziale Medien und die DSGVO: Recht auf Auskunft und Datenübertragbarkeit', Die Marktwächter, accessed 13 May 2020, https://www.marktwaechter.de/digitale-welt/marktbeobachtung/soziale-medien-und-die-dsgvo-recht-auf-auskunft-und-datenuebertragbarkeit.

74 Marktwächter Digitale Welt, 'Soziale Medien Un Die EU-Datenschutzgrundverordnung - Teil II', chaps 4–5.

75 Streaming Services', Noyb.Eu, accessed 12 May 2020, https://noyb.eu/en/project/streaming-services.

reasons. First, responses to access requests often do not contain all the personal data that is being collected. This argument is based on the observation that data which is explicitly mentioned in the privacy policy is not provided in response to the access request. Moreover, there is reason to believe that other information is missing as well, but the data subject is not in the position to prove this. Therefore, the complaint asks the DPA to investigate the company. Second, responses also often lack other information that needs to be provided such as information about purposes, recipients and sources. Third, the complaints allege that responses contain information which is not intelligible.

The complaints request a number of actions by the DPAs. First, to investigate the complaint, including to determine which data is held by the data controller. Second, to find a violation of the right of access. Third, to compel the controller to comply fully with the request. Fourth, to impose an appropriate fine.

1.9. Schrems v Facebook

- *Location*: Europe
- *Time*: 2011-ongoing
- *One-liner*: multiple procedures against Facebook
- *Driving force*: civil society (Max Schrems, Europe-v-facebook.org and fbclaim.com)
- *Goal*: holding Facebook to account, investigating whether data protection rights are enforceable.
- *Est. number of participants*: over 60.000

In 2011 Max Schrems, then a law student, asked Facebook for the data it held about him. He received 1200 pages of data and published this on the website Europe-v-facebook.org.[76] On this website he also shared information about what data Facebook has and how to request it.[77] On the basis of the response to his request he filed 22 complainst at the Irish data protection authority. After 3 years he retracted most claims, citing the refusal to provide a formal decision and lack of procedural rights, and the fact that the costs of litigating against the DPA would have been to high.[78] He concluded that "no normal citizen is able to follow through with such a proceeding". However, Schrems was able to continue with one case, financed through the collection of donations, targeting the transfer of his personal data outside Europe. In October 2015, the Court of Justice of the EU famously ruled amongst other things that the Safe Harbor rules are invalid.[79]

In 2014 Schrems started a procedure against Facebook in Austria based on the complaints that the Irish DPA had not decided on.[80] The case was started as a class action with the number of participants was limited to 25.000 people, although 60.000 people responded to his call.[81] However, in 2018 The Court of Justice ruled that Schrems could only file an individual

76 Olivia Solon, 'How Much Data Did Facebook Have on One Man? 1,200 Pages of Data in 57 Categories', Wired UK, 28 December 2012, https://www.wired.co.uk/article/privacy-versus-facebook.

77 'Europe-v-Facebook Data Pool', europe-v-facebook.org, accessed 13 May 2020, http://europe-v-facebook.org/EN/Data_Pool/data_pool.html.

78 'Europe-v-Facebook Complaints', europe-v-facebook.org, accessed 13 May 2020, http://europe-v-facebook.org/EN/Complaints/complaints.html.

79 CJEU Judgement of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650

80 http://www.europe-v-facebook.org/sk/CJEU_en.pdf

claim but no class action.[82] The case is currently still ongoing at the Vienna Regional Court for Civil Matters.[83]

1.10. Twitter

- *Location*: international, UK
- *Time*: 2012
- *One-liner*: collectively asking Twitter for personal data
- *Driving force*: civil society (Privacy International)
- *Goal*: raising awareness and gaining clarity on what information Twitter stores
- *Est. number of participants*: unknown

In response to news about Twitter's data collection (notably of phone contacts) and the sharing of Twitter data with United States enforcement officials, Privacy International started a campaign targeting Twitter.[84] It encouraged people to ask Twitter what information the company held on them.[85] The website of Privacy International included instructions on how to request the data, a sample text and instructions on the further procedure. Privacy International also asked people to pay attention to Twitter's retention period about its data subjects and to report in case people find odd or missing results.

2. Safeguarding other Fundamental Rights

2.1. Discrimination in college admissions

- *Location*: US (Stanford University)
- *Time*: 2015
- *One-liner*: students use access right under FERPA to obtain information about the admissions procedure of Stanford University
- *Driving force*: students
- *Goal*: uncovering potentially discriminatory practices, revealing admission criteria
- *Est. number of participants*: 2000[86]

---

81 Ingrid Lunden, 'European Facebook Class Action Suit Attracts 60K Users As It Passes First Court Hurdle', accessed 13 May 2020, https://techcrunch.com/2014/08/21/european-facebook-class-action-suit-attracts-60k-users-as-it-passes-first-court-hurdle/.

82 CJEU Judgement of 25 January 2018, *Maximilian Schrems v Facebook Ireland Limited*, C498/16, ECLI:EU:C:2018:37

83 noyb. (2020, February 26). Facebook witness: 9 ½ hours of "we don't know." Noyb.Eu. https://noyb.eu/en/facebook-witness-9-12-hours-we-dont-know

84 David Sarno, 'Twitter Stores Full IPhone Contact List for 18 Months, after Scan', Los Angeles Times, 14 February 2012, https://www.latimes.com/business/la-xpm-2012-feb-14-la-fi-tn-twitter-contacts-20120214-story.html; Quinn Norton, 'Boston D.A. Subpoenas Twitter Over Occupy Boston, Anonymous', Wired, 30 December 2011, https://www.wired.com/2011/12/boston-subpoena-twitter/.

85 Privacy International, 'What Does Twitter Know about Its Users? #NOLOGS', accessed 13 May 2020, http://www.privacyinternational.org/blog/1504/what-does-twitter-know-about-its-users-nologs; Andreas Müller, 'Was weiß Twitter über dich? Verlange Auskunft!', Netzpolitik.org, accessed 13 May 2020, https://netzpolitik.org/2012/was-weis-twitter-uber-dich-verlange-auskunft/.

The Fountain Hopper, a student-run newsletter, called upon fellow students at Stanford to exercise their subject access right under the Family and Educational Rights and Privacy Act (FERPA) in 2015.[87] The aim was to obtain access to documents relating to their educational record, which includes their admission files.[88] Students wanted to know what the criteria are for admission and to what extend race plays a role. Stanford students would receive detailed instructions on how to file a request. Over 2000 students requested their files.[89] This, in turn, inspired students at other selective colleges to follow suit, and file requests at their universities.

2.2. Discrimination in credit scoring: OpenSchufa

- *Location*: Germany
- *Time*: 2018-2019
- *One-liner*: collectively reverse-engineering credit-scoring algorithms
- *Driving force*: civil society (algorithm watch and OKF) journalism (Bayerischer Rundfunk and Spiegel)
- *Goal*: understanding automated decision making

Schufa is the largest credit scoring agency in Germany. Its scores are used to determine if people can get a loan, a call phone contract and even rent an apartment. Civil society organisations have long demanded that there should be transparency about how this score is calculated. Citizens have individually used the right of access to gain insight into their score, and on how their score was calculated. In response to access requests, Schufa provided access to the personal data that was used to calculate the score, as well as to the score itself. In 2014 the Bundesgerichtshof (German supreme court) in a case against Schufa decided that the individual did not have a right to know the weights of the elements in the determination of the score, nor information on comparison groups.[90]

NGOs Algorithm Watch and Open Knowledge Foundation Deutschland ran a campaign "OpenSCHUFA" based on access requests to create and demand transparency on the functioning of Schufa's credit scoring algorithm.[91] Approximately 4,000 people shared the response to an access request with the NGOs. Based on the personal data and credit scores contained in those responses they reverse engineered the scoring algorithm. Due to the relatively small selection (compared to the overall number of people in Schufa's database), only a limited number of results could be drawn.

---

86 'Fight Back with FERPA', *The Fountain Hopper*, 14 December 2016, https://us9.campaign-archive.com/?u=c9d7a555374df02a66219b578&id=4f634ec27c&e=881def51bf.

87 'How To Get Your Internal Stanford Admissions File (Or: What They Really Thought Of You)', The Fountain Hopper, 15 January 2015, https://us9.campaign-archive.com/?u=c9d7a555374df02a66219b578&id=3a69d6c439.

88 Molly Hensley-Clancy, 'Here's How To See What College Admissions Officers Wrote About You', BuzzFeed News, accessed 13 May 2020, https://www.buzzfeednews.com/article/mollyhensleyclancy/heres-how-to-see-what-college-admissions-officers-wrote-abou.

89 Richard Pérez-Peña, 'Students Gain Access to Files on Admission to Stanford', The New York Times, 16 January 2015, sec. U.S., https://www.nytimes.com/2015/01/17/us/students-gain-access-to-files-on-admission-to-stanford.html.

90 Bundesgerichtshof, 'Pressemitteilung Nr. 16/14', 28 January 2014, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2014&Sort=3&nr=66583&pos=1&anz=17.

91 Bundesgerichtshof, 'Pressemitteilung Nr. 16/14', 28 January 2014, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2014&Sort=3&nr=66583&pos=1&anz=17.

2.3. *Price discrimination: Personalised pricing*

- *Location*: Netherlands
- *Time*: 2014-2016
- *One-liner*: research into the practice of personalised pricing
- *Driving force*: civil society (Bits of Freedom)
- *Goal*: revealing whether companies use personalised pricing
- *Est. number of participants*: 50

After information surfaced that companies in the United States applied personalized pricing, the Dutch digital rights organization Bits of Freedom started an inquiry with regards to the Dutch market.[92] It wanted to know to what extent personalised pricing is used in the Netherlands.[93] Bits of Freedom sent subject access requests to various organisations, such as online stores, travel agencies and insurance companies. The request asked for personal information collected and whether the companies applied personalised pricing. The information obtained through the subject access requests was combined with an empirical study, in which screenshots of webpages were made and compared. Bits of Freedom concluded that the companies collect vast amounts of data and that it is difficult to receive information about personalised pricing. Different users got to see different prices for the products, but it was unclear whether this was the result of personalised pricing. Furthermore, Bits of Freedom noted that most – but not all – companies responded in time to the requests, but the quality of the responses varied greatly.[94]

2.4. *Fair elections: Political microtargeting*

- *Location*: international, but especially UK and US
- *Time*: 2018-…
- *One-liner*: using transparency measures – including access requests – in order to better understand (political) ad targeting and hold industry accountable
- *Driving force*: journalism and civil society
- *Goal*: uncovering issues and holding accountable relevant actors

Over the last years legal transparency requirements (and to some extent the right of access) have played a central role in investigating the role of micro-targeting in the context of elections and its growing impact on democratic institutions. Either by directly exercising the right[95] and/or through transparency-tools that have been produced by companies in

92 Jennifer Valentino-DeVries Soltani Jeremy Singer-Vine and Ashkan, Jeremy Singer-Vine, and Ashkan Soltani, 'Websites Vary Prices, Deals Based on Users' Information', Wall Street Journal, 24 December 2012, https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

93 Floris Kreiken, 'Personalisering: van promotie tot prijs', Bits of Freedom, accessed 13 May 2020, https://www.bitsoffreedom.nl/2016/05/18/personalisering-van-promotie-tot-prijs/.

94 Floris Kreiken, 'Personalisering: Van Promotie Tot Prijs' (Bits of Freedom, 26 April 2016), https://www.bitsoffreedom.nl/wp-content/uploads/20160426-bits-of-freedom-personalisering-van-promotie-tot-prijs.pdf.

95 Carole Cadwalladr, 'Arron Banks, the Insurers and My Strange Data Trail', The Guardian, 21 April 2018, sec. Technology, https://www.theguardian.com/technology/2018/apr/21/arron-banks-insurance-personal-data-leave-eu; Carole Cadwalladr, 'UK Regulator Orders Cambridge Analytica to Release Data on US Voter', The Guardian, 5 May 2018, sec. UK news, https://www.theguardian.com/uk-news/2018/may/05/cambridge-analytica-uk-regulator-release-data-us-voter-david-carroll.

accommodating legal/policy requirements (not limited to GDPR) or even independently generated databases.[96]

In 2017 the US citizen Prof. David Caroll requested his data from Cambridge Analytica. Caroll received a portion of the data Cambridge Analytica held on him, but expected that this was not all information they had on him. In order to shed light on Cambridge Analytica's practices he filed a complaint at the UK Information Commissioner's Office.[97] The ICO ruled in his favor, but Cambridge Analytica did not comply. A district court eventually fined the company as it failed to comply with the order. Failure to comply with (an ICO enforcement notice to accommodate) an access request by Cambridge Analytica also resulted in criminal proceedings.[98] A day before this ruling, the company went into administration.[99]

2.5. Fair elections: UK General Elections

- *Location*: UK
- *Time*: 2019
- *One-liner*: revealing information about political targeting by UK political parties.
- *Driving force*: civil society (Open Rights Group)
- *Goal*: finding out how personal data is used by political parties to profile voters
- *Est. number of participants*: >1,000

Before the UK General Elections of 2019, Open Rights Group started a campaign to find out how political parties use voters' personal data. It called on the general public to submit subject access requests and provided a tool to do so.[100] It received thousands of responses.[101] One of the findings is that all three major parties in the UK are collecting personal data and using this to profile voters.[102] Open Rights Group used this research also as part of the basis for its oral evidence in the All Party Parliamentary Group on Electoral Campaigning

96 Julia Carrie Wong, 'One Year inside Trump's Monumental Facebook Campaign', The Guardian, 29 January 2020, https://www.theguardian.com/us-news/2020/jan/28/donald-trump-facebook-ad-campaign-2020-election; Julia Carrie Wong, Michael Barton, and Joseph Smith, '$45m, 1.6bn Views and "Crazy Donald": How Bloomberg Bought Your Facebook Feed', The Guardian, 21 February 2020, https://www.theguardian.com/us-news/2020/feb/21/mike-bloomberg-facebook-ad-campaign; Jeremy B. Merill, 'What We Learned From Collecting 100,000 Targeted Facebook Ads — ProPublica', ProPublca, accessed 12 May 2020, https://www.propublica.org/article/facebook-political-ad-collector-targeted-ads-what-we-learned.

97 David Carroll, 'Why I Took Legal Action Against Cambridge Analytica', Vice, accessed 12 May 2020, https://www.vice.com/en_us/article/d35vym/david-carroll-cambridge-analytica-facebook-legal-claim.

98 Information Commissioner's Office (UK), 'SCL Elections Prosecuted for Failing to Comply with Enforcement Notice', 11 January 2019, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/01/scl-elections-prosecuted-for-failing-to-comply-with-enforcement-notice/.

99 CA Commercial, 'Cambridge Analytica and Scl Elections Commence Insolvency Proceedings and Release Results of Independent Investigation into Recent Allegations', accessed 12 May 2020, https://web.archive.org/web/20180502183542/https://ca-commercial.com/news/cambridge-analytica-and-scl-elections-commence-insolvency-proceedings-and-release-results-3.

100 Open Rights Group, 'Who Do Political Parties Think We Are?', accessed 13 May 2020, https://action.openrightsgroup.org/who-do-political-parties-think-we-are-4.

101 Open RIghts Group, 'Open Rights Group February 2020 Newsletter', accessed 13 May 2020, https://www.openrightsgroup.org/support-org/february-2020-newsletter/.

102 Matthew Rice, 'What We've Learned from Asking Political Parties: Who Do You Think We Are?', Open Rights Group, 3 December 2019, https://www.openrightsgroup.org/blog/2019/what-weve-learned-from-asking-political-parties:-who-do-you-think-we-are.

Transparency.[103] Together with several other NGOs it wrote a briefing on the digital landscape around the elections and called for a change in the laws.[104] Furthermore, Open Rights Group has written pre-action letters to the three main political parties based on the received documents.[105]

2.6. Labour rights: FairTube

- *Location*: international
- *Time*: 2019
- *One-liner*: content-creators seeking more transparency and a fair treatment from Youtube (notably regarding de-monetisation and recommender systems)
- *Driving force*: Youtubers, civil society
- *Goal*: creating social justice

In 2019, a number of (semi-)professional youtubers that relied on advertisement income set up FairTube.[106] The campaign is aimed at forcing fairer and more transparent decision-making processes on the (de-)monetisation of content by YouTube. For this, collaboration was sought with IG Metall (the biggest workers union in Germany). As part of their efforts, FairTube seeks to enable access for content-creators, to the data and decision-making procedures that YouTube uses to determine the (de-)monetisation.[107]

2.7. Labour rights: Uber drivers

- *Location*: UK
- *Time*: 2018-…
- *One-liner*: gig-economy workers using data rights to force better working conditions (e.g. minimum wages, challenge abusive algorithmic management, etc.)
- *Driving force*: civil society, workers
- *Goal*: social justice

The so-called platform/gig economy, has a massive impact on labour rights and social justice more broadly.[108] Access rights are used by various labour rights movements, in particular in the platform economy. One example is labour union Worker Info Exchange, which uses the

---

103 Pascal Crowe, 'APPG on Electoral Campaigning Transparency Adopt ORG Reforms to Electoral Landscape', Open Rights Group, 31 January 2020, https://www.openrightsgroup.org/blog/2020/appg-on-electoral-campaigning-transparency-adopt-org-reforms-to-electoral-landscape.

104 Computational Propaganda Project, University of Oxford et al., 'UK General Election 2019: Digital Disruption by the Political Parties, and the Need for New Rules', December 2019, https://www.isdglobal.org/wp-content/uploads/2019/12/UK-GE-2019-Digital-Disruption-report.pdf.

105 Open RIghts Group, 'Campaigners Demand Answers over Parties Use of Personal Data in General Election', accessed 13 May 2020, https://www.openrightsgroup.org/press/releases/2019/campaigners-demand-answers-over-parties-use-of-personal-data-in-general-election.

106 FairTube, 'FairTube Campaign: For Fairness and Transparency for All YouTube Creators', accessed 12 May 2020, https://fairtube.info/en/.

107 Edward Ongweso, 'The YouTubers Union Is Not Messing Around', Vice, 26 July 2019, https://www.vice.com/en_us/article/j5wy8d/the-youtubers-union-is-not-messing-around.

108 Privacy International, 'Case Study: The Gig Economy and Exploitation', Privacy International, accessed 12 May 2020, http://privacyinternational.org/case-study/751/case-study-gig-economy-and-exploitation.

right of access for Uber drivers to get access to the data that Uber holds on them.[109] Drivers currently do not have access to basic data such as their log-off/on times to the platform (necessary in order to calculate the effective hourly income). Getting access to their data is a way to balance the information-driven power asymmetry between drivers and the company. Eventually this could support their fight for fundamental labour rights such as minimum wage.

Similar efforts might be useful in many other places where workforces are algorithmically (micro-)managed, from platforms-economy operators (eg. Deliveroo and Mechanical Turk)[110] to more traditional companies.[111]

2.8. Unfair commercial practices: Dexia bank

- *Location*: Netherlands
- *Time*: from 2004-2019
- *One-liner*: consumer tv programme calls on clients from a bank to ask for their personal information
- *Driving force*: journalism, civil society
- *Goal*: collecting data to proove malfeasance by Dexia bank
- *Est. number of participants*: over 3800

To understand the relevance of this case it is important to know that one particular aspect of the Dutch financial landscape before the financial crises of 2008 was that, spurred by specific fiscal rules, financial institutions had started to sell complex and risky products to the general public. A popular consumer protection television programme, Radar, advised clients of banks who had bought such products to file access requests to acquire data that could help prove the wrongdoing by the banks in court, and provided the template for such request. Against this background, thousands of clients used their right of access to request data from Dexia, one of the banks that had sold these financial products. The clients requested their complete file including in particular a copy of the contracts between the clients and the bank, their risk profile and a transcription of recordings the bank made of telephone conversations it had with the clients. The files obtained through the access requests were later used in class action lawsuits against the financial institutions.

---

109 Open Society Foundations, 'Q&A: Workers Have a Right to Know', accessed 12 May 2020, https://www.opensocietyfoundations.org/voices/q-and-a-fighting-for-workers-right-to-data; 'Uber Drivers Demand Their Data', The Economist, 20 March 2019, https://www.economist.com/britain/2019/03/20/uber-drivers-demand-their-data; 'Worker Info Exchange – Data Rights for Digital Workers', accessed 12 May 2020, https://workerinfoexchange.org/.

110 Xuefei Deng, Kshiti D. Joshi, and Robert D. Galliers, 'The Duality of Empowerment and Marginalization in Microtask Crowdsourcing: Giving Voice to the Less Powerful through Value Sensitive Design', Mis Quarterly 40, no. 2 (2016): 279–302.

111 Mareike Möhlmann and Ola Henfridsson, 'What People Hate About Being Managed by Algorithms, According to a Study of Uber Drivers', Harvard Business Review, 30 August 2019, https://hbr.org/2019/08/what-people-hate-about-being-managed-by-algorithms-according-to-a-study-of-uber-drivers.

3. Investigative Journalism

3.1. Amazon

- *Location*: UK
- *Time*: 2019-2020
- *One-liner*: journalist want to reveal what data Amazon stores though its Ring devices
- *Driving force*: journalism
- *Goal*: raising awareness and creating public accountability
- *Est. number of participants*: 1

A journalist from the BBC filed an access request to learn about the data collected through Amazon Ring,[112] as part of a wider investigation into what information Amazon collects and uses.[113] In the initial response to the access request Amazon did not elaborate what information is was gathering, apart from what was stated in the privacy notice. According to the BBC, the privacy notice was worded in inexact terms. Eventually, access to detailed data from 11 databases was provided, which included every interaction with the doorbell or its app, every motion it detects, the type of phone used to interact with it, whether you zoom in on something, the duration of each interaction, as well as the geo-location were the device is installed.

3.2. Comparing responses to access requests sent from UK and US

- *Location*: UK and US
- *Time*: 2018
- *One-liner*: two reporters, one from the UK and one from the US send access requests to seven companies, to compare the level of access between the two countries
- *Driving force*: journalism
- *Goal*: raising awareness and creating public accountability

In an article for the *New York Times*, two reporters, one from the UK and one from the US sent access requests to seven companies, to compare the level of access between the two countries where the UK has a broad data protection law providing a general right of access to personal data and the US does not.[114] They found that two companies (Quantcast and Amazon) provided more information to the UK reporter. For other companies (Facebook, Twitter and LinkedIn) who rely on a data download tool, the response was exactly the same. Other than giving limited access through the data download tool, no further information was given. They note that: 'researchers, journalists and consumers have been seeking their personal details from companies to try to understand how we might be manipulated. The incomplete responses from tech companies do not bode well for such research efforts.'

112 Leo Kelion, 'Ring Logs Every Doorbell Press and App Action', BBC News, 4 March 2020, https://www.bbc.com/news/technology-51709247.

113 Kelion, Leo. "Amazon: Why Amazon Knows so Much about You." BBC News (blog), 2020. https://bbc.co.uk/news/extra/CLQYZENMBI/amazon-data.

114 Natasha Singer and Prashant S. Rao, 'U.K. vs. U.S.: How Much of Your Personal Data Can You Get?', The New York Times, 20 May 2018.

3.3. *eReaders*

- *Location*: US
- *Time*: 2020
- *One-liner*: journalist files access request with Amazon under new California privacy act, and discovers the extent of data collection and processing of their reading behavior
- *Driving force*: journalism
- *Goal*: raising awareness and creating public accountability

Right after the new California privacy act entered into force, a Guardian journalist filed access requests to obtain their Kindle data. It included not just their order history, shipping information and customer support chat logs, but also two Excel spreadsheets containing more than 20,000 lines each, with titles, time stamps and actions detailing the journalist's reading habits on the Kindle app.

3.4. *Facebook contact import*

- *Location*: France
- *Time*: 2019
- *One-liner*: journalist goes on a quest to find out how companies target her on Facebook
- *Driving force*: journalism
- *Goal*: finding out more about data sharing practices on Facebook
- *Est. number of participants*: 1

Perrine Signoret, a journalist from the French news website Numerama, dives into her Facebook profile and finds a list of companies that have imported a contact list in which she appears.[115] The list contained many companies she did not have a relation with, and she wondered how they had obtained her contact details. She sent the companies on the list subject access requests. She wanted to know if the companies held any information on her and how they obtained this information. Some of the companies only responded to her data access requests after she revealed herself as a journalist. Some companies did not respond at all. The companies often said they do not hold any information on her, pointing toward Facebook to find out more. After a while she received a response from a company that explains that they had acquired the information through one of their partner companies. She wondered if that is how all the companies appeared on the list, but because most companies did not say they had the information she could not dive deeper. Four months later she wrote a follow-up article.[116] In response to the previous article companies had contacted her and provided her with more information. It turned out that many of the companies had made use of the services of a company named LiveRamp. She requested her personal data from LiveRamp. It turns out that her email address has been used linked to another person's name and obtained because somebody filled out a consumer survey.

115 Perrine Signoret, 'J'ai voulu savoir qui avait vendu mes données personnelles et je suis tombée dans un puits sans fond', Numerama, accessed 12 May 2020, https://www.numerama.com/tech/476311-jai-voulu-savoir-qui-avait-vendu-mes-donnees-personnelles-et-je-suis-tombee-dans-un-puits-sans-fond.html.

116 Perrine Signoret, 'J'ai (enfin) découvert pourquoi des marques inconnues me ciblaient sur Facebook', Numerama, accessed 12 May 2020, https://www.numerama.com/tech/508381-jai-enfin-decouvert-pourquoi-des-marques-inconnues-me-ciblaient-sur-facebook.html.

3.5. *Facebook's Off-Facebook activity tool*

- *Location*: Europe
- *Time*: 2020
- *One-liner*: journalist tries to find out more about the data that is not included in Facebook's "Offline activity tool"
- *Driving force*: journalism
- *Goal*: illustrating how Facebook's tool does not provide all the information Facebook holds on a given person
- *Est. number of participants*: 1

Early 2020 Facebook made a tool available to all its users that promises to give more control to users about what information Facebook received through third parties and delete that too.[117] Natasha Lomas, journalist for TechCrunch, used this tool and illustrates what information is missing.[118] In addition, she reaches out to the companies that shared data with Facebook and Facebook itself. She inquired with these companies about the data collection as a journalist. The article shows how much is unknown after using Facebook's Off-Facebook activity tool.

3.6. *Location-data and smartphone apps*

- *Location*: Netherlands
- *Time*: 2019
- *One-liner*: journalists filing requests with popular smartphone apps to demonstrate the scale and sensitivity of location-tracking
- *Driving force*: journalism
- *Goal*: raising awareness and creating public accountability

Dutch journalists looked at the use of location data by the most used iPhone apps in the Netherlands.[119] They downloaded the apps, used them, and then sent out subject access requests to the respective companies. They found that some apps only process location data on the phone, while other send the location data back to central servers. Some companies at first claim they do not hold such data, even though the apps do request permission to location data. When journalists uncover themselves as such, companies admit that they do process location data.

3.7. *Oli Frost*

- *Location*: UK

---

117 Mark Zuckerberg, 'Starting the Decade by Giving You More Control Over Your Privacy', Starting the Decade by Giving You More Control Over Your Privacy, accessed 13 May 2020, https://about.fb.com/news/2020/01/data-privacy-day-2020/.

118 Natasha Lomas, 'Facebook's Latest "Transparency" Tool Doesn't Offer Much — so We Went Digging', TechCrunch, 25 February 2020, https://social.techcrunch.com/2020/02/25/facebooks-latest-transparency-tool-doesnt-offer-much-so-we-went-digging/.

119 Anouk Burgman, Eric Van den Berg, and Eric San Giorgi, 'Anouk Ging Naar Een Abortuskliniek. Een Bekende App Wist Daarvan En Verkocht Die Informatie', https://www.npo3.nl/brandpuntplus/anouk-ging-naar-een-abortuskliniek-een-bekende-app-wist-daarvan-en-verkocht-die-informatie, accessed 13 May 2020.

- *Time*: 2018
- *One-liner*: British satirist puts his Facebook data up for sale to the highest bidder
- *Driving force*: satire (Oli Frost)
- *Goal*: drawing attention to the marketing of personal data, satire
- *Est. number of participants*: 1

The British satirist Oli Frost put his personal data for sale on Ebay.[120] In interviews he explained that Facebook had been making money with this data for years, why should he not?[121] He had downloaded the personal data Facebook had on him through Facebook's download your data tool.[122] The eBay advertisment illustrates what type of information he is selling, such as "who I vote for, my boss's name, and where all my family live" and "A list of things I'm apparently interested in, including 'Gluten-free diet', 'Jessie Ware' and 'Project management software'". The advertisement further stipulates that the buyer can sell it to other advertisers but is not allowed to steal Oli Frosts' identity. The proceeds would go to the Electronic Frontier Foundation. The bidding started at 99 cents, but the price went up rapidly to £300,-.[123] At that point Ebay took the advertisement down, claiming that selling this information could be a violation of Facebook's terms of service.[124] Oli Frost responds on his website: "My mistake, I was under the impression I owned my personal data".[125]

3.8. Opération Data

- *Location*: Switzerland
- *Time*: 2020
- *One-liner*: journalistic project based on subject access request to reveal data practices
- *Driving force*: journalism (Le Temps)
- *Goal*: informing the public about data surveillance
- *Est. number of participants*: 50

In the beginning of 2020, the Swiss newspaper Le Temps commenced a project to shed light on the data practices of companies together with Paul-Olivier Dehaye from personaldata.io.[126] The newspaper asked its readers to participate in this project. A small group of readers was guided through the process of requesting access to their personal data from various

120 Oli Frost gained media attention for other projects before, often to attract attention to social issues: Oli Frost's website, accessed 13 May 2020, https://olifro.st/.

121 Tom Usher, 'Man Tried to Sell All His Facebook Data on EBay for £300', Metro, accessed 13 May 2020, https://metro.co.uk/2018/05/31/man-tried-to-sell-all-his-facebook-data-on-ebay-for-300-7595007/; Patrick Lucas Austin, 'A Man Is Auctioning His Facebook Data on EBay, and It's Going Great [Update: Not Anymore]', Gizmodo, accessed 13 May 2020, https://gizmodo.com/a-man-is-auctioning-his-facebook-data-on-ebay-and-its-1826389102.

122 Oli Frost, 'I Put All My Personal Facebook Data on EBay', Oli Frost's Website, 27 May 2018, https://olifro.st/blog/data-on-ebay/.

123 Daniel Oberhaus, 'This Guy Is Selling All His Facebook Data on EBay', Vice, accessed 13 May 2020, https://www.vice.com/en_uk/article/3k4ay8/sell-facebook-data-ebay-oli-frost.

124 Gael Fashingbauer Cooper, 'You Can Buy This Guy's Personal Facebook Data, Just Not on EBay', CNET, accessed 13 May 2020, https://www.cnet.com/news/you-can-buy-oli-frost-personal-facebook-data-just-not-on-ebay/.

125 Frost, 'I Put All My Personal Facebook Data on Ebay'.

126 Florian Delafoi and Paul Ronga, 'Reprenez le contrôle de vos données! «Le Temps» propose une expérience participative', Le Temps, 7 January 2020, https://www.letemps.ch/societe/reprenez-controle-vos-donnees-temps-propose-une-experience-participative.

organisations and deciphering the information received.[127] The project is hoped to form the basis for future news articles. As the project starts, a Swiss data protection law is discussed in Parliament.

3.9. Tinder

- *Location*: France
- *Time*: 2017-2019
- *One-liner*: through access requests and other sources, a journalist explores the impact of algorithmic dating in online dating apps, uncovering the scale of data processing, recommender systems, and a 'desirability score'
- *Driving force*: journalism
- *Goal*: cracking the black box, societal impact

Journalist Judith Duportail investigated the data collection and algorithmic decision making by Tinder. As part of her investigation she filed access requests with the help of Paul-Olivier Dehaye of personaldata.io and solicitor Ravi Naik. She received 800 pages of information, including among other things the people she matched with, the number of times she opened the app, Instagram photos, location and time of every conversation. Apart from many newspaper articles, Duportail also published her findings in a book.[128] Duportail discusses how people are lured into sharing data with Tinder without being aware of its implications. She recounts how receiving all of her data in response to her access request was a very sobering experience. Tinder extensively uses data for feeding its recommender/matching algorithm but fails to explain how their algorithm works (mainly relying on their intellectual property rights as a defence). For the book that was published 2 years after the Guardian article, Duportail builds on information from many more sources. In particular, she argues that most probably a desirability score is used in the app because she found a patent for such a score filed by the co-founders of the app.

In another article, Dehaye recounts how, under the Data Protection Directive, Tinder – as an American company – could not be forced to respond to an access request.[129] Therefore the response given to Duportail by Tinder was in some sense voluntary. It seems that the fact that the request came from a journalist put some pressure on the company, as others who have sent access request to Tinder have not received the same amount of information.

3.10. Wizards Unite

- *Location*: Europe
- *Time*: 2019

---

127 Florian Delafoi, 'Données personnelles: «Nous devons étendre le champ de la transparence»', Le Temps, 23 January 2020, https://www.letemps.ch/economie/donnees-personnelles-devons-etendre-champ-transparence.

128 Judith Duportail, 'I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets', The Guardian, 26 September 2017, https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold; Duportail.

129 Paul-Olivier Dehaye, 'Getting Your Data out of Tinder Is Hard. It Shouldn't Be', The Guardian, 27 September 2017, https://www.theguardian.com/technology/2017/sep/27/tinder-data-privacy-tech-eu-general-data-protection-regulation.

- *One-liner*: gaming journalists look into how much location data is stored when playing Wizards Unite
- *Driving force*: journalism (Kotaku)
- *Goal*: gaining insight into how much data is recorded when playing Wizards Unite and illustrating the value of location data to companies
- *Est. number of participants*: 10

Game news website Kotaku asked European players of Wizards Unite, an augmented reality game created by Niantic, to request their personal data and share the outcomes with Kotaku.[130] Ten players responded. The files contained a wide range of information, such as the estimated amount of calories players burned, promotions they signed up for and location data. After analysing the data, over 25,000 location records, they concluded that the Niantic kept about three location records per minute of gameplay. The article further shows how much information can be derived from the location data and how tech companies create revenue from this.

4. Tools to facilitate the exercise of data subject rights

Several organisations provide tools aimed at helping individuals to use their data subject rights and in particular the right of access. All of these provide template letters, and some provide additional functionality such as providing lists of contact details where access requests can be directed to, as well as giving reminders at end of the maximum period data controllers have to respond to requests.

Organisations that build these tools do this for multiple reasons. The primary goals are to raise awareness about data subject rights as well as about privacy and data protection in general, and to facilitate campaigns. They are further picked up by other actors such as journalists and academics.

4.1. MyDataDoneRight

MyDataDoneRight is a tool developed by Bits of Freedom, a digital rights organisation in the Netherlands.[131] It was launched in 2018 around the time of the introduction of the GDPR. The tool is currently available three languages – English, French and Dutch – and through partnerships with local NGOs will be made available across Europe, supporting local languages and including localised contact lists.

Bits of Freedom also regularly publishes blog posts about the use of data subject rights and MyDataDoneRight (in Dutch).[132] In these posts various issues are discussed such as which barriers to the effective use of the rights users have experienced and whether these are legal, and the organisation of community meetings to add and correct entries to the database of data controllers.

130 Cecilia D'Anastasio and Dhruv Mehrotra, 'The Creators Of Pokémon Go Mapped The World. Now They're Mapping You', Kotaku, accessed 13 May 2020, https://kotaku.com/the-creators-of-pokemon-go-mapped-the-world-now-theyre-1838974714.

131 https://www.mydatadoneright.eu/. Replacing their previous tool called Privacy Inzage Machine (PIM), launched in 2011.

132 'My Data Done Right examples', Bits of Freedom, accessed 13 May 2020, https://www.bitsoffreedom.nl/tag/my-data-done-right/.

Journalists have used the tool to support privacy and data protection awareness campaigns. For example, two Dutch journalists invited their readers to collectively file access requests with the tax authority.[133] They explain that people can use PIM/MyDataDoneRight for this. They chose the tax authority because they see it as "the biggest information factory" of the country and even wanted to expand their use of personal data. They also believe that massively sending an access request gives a signal to the tax authority that people care about privacy and the protection of their data.

In 2019 blogger 'JerryHopper' posted about the neighborhood hub app 'Nextdoor'. In his posts he revealed how to get access to closed neighborhood groups and by extension access to the personal data of the people in the groups, by falsifying address data.[134] When a consumer television programme reported on this, they invited digital rights group Bits of Freedom to their show.[135] Bits of Freedom called on people to request their data and ask for removal.[136] Approximately 6000 people did with the help of the MyDataDoneRight tool.[137]

4.2. Access My Info

Access My Info, released in 2014, is an online access request letter generator created by Citizen Lab in Canada and has been localised for Canada and Hong Kong.[138] Contrary to most other tools, it provides specific templates for access requests letters in specific industries (telecommunication, dating applications and fitness trackers). The templates provided through Access My Info refer to specific categories of data, depending on the sector. For example, while letters to mobile operators specifically request access to call logs, requests to fitness trackers specifically request access to health data). At the time of writing the Canadian version has been used around 8,000 times and the Hong Kong version about 2,000 times.

The goal of the project is to "enhance transparency" by helping citizens to (1) "obtain some answers from companies about their data retention, management, and disclosure policies" and

133 Dimitri Tokmetzis and Maurits Martijn, 'Vraag vandaag wat de Belastingdienst allemaal over jou weet #privacyweek', De Correspondent, accessed 13 May 2020, https://decorrespondent.nl/5990/vraag-vandaag-wat-de-belastingdienst-allemaal-over-jou-weet-privacyweek/291695030-93fe3e34.

134 Jerry Hopper, 'Nextdoor lekt uw NAW gegevens', For your information, accessed 14 May 2020, https://foryourinformation.nl/2019/07/25/nextdoor-lekt-uw-naw-gegevens/; Jerry Hopper, 'Nextdoor (2) - BuurtApp', For your information, accessed 14 May 2020, https://foryourinformation.nl/2019/07/30/nextdoor-buurtapp-deel-2/.

135 Douwe Schmidt, 'Gratis af te halen bij Marktplaats: persoonsgegevens van derden', De Correspondent, accessed 13 May 2020, https://decorrespondent.nl/1251/gratis-af-te-halen-bij-marktplaats-persoonsgegevens-van-derden/48601292454-afe96caa.

136 Stijn Bronzwaer, 'Buurtapp Nextdoor in opspraak: duizenden leden vragen hun data op', NRC, 23 September 2019, https://www.nrc.nl/nieuws/2019/09/23/buurtapp-nextdoor-in-opspraak-duizenden-leden-vragen-hun-data-op-a3974348; Avrotros Radar, 'Nextdoor en privacy: 11 vragen en antwoorden', accessed 14 May 2020, https://radar.avrotros.nl/hulp-tips/hulpartikelen/item/nextdoor-en-privacy-11-vragen-en-antwoorden/.

137 Tijdelijke commissie Digitale Toekomst, 'Conceptverslag Openbare kennisbijeenkomst' (Tweede Kamer der Staten Generaal, 23 September 2019), 63, https://www.tweedekamer.nl/kamerstukken/detail/2019D39723/2019D39723.

138 'Access My Info', accessed 13 May 2020, https://accessmyinfo.org/; 'Access My Info (Canada)', accessed 13 May 2020, https://accessmyinfo.ca/#home; 'Access My Info (Hong Kong)', accessed 13 May 2020, https://accessmyinfo.hk/#home.

(2) to "function as a means for Canadians to demonstrate their concerns about how their data was handled."[139]

4.3. Personaldata.io

Personaldata.io[140] is an organisation promoting digital rights founded by Paul-Olivier Dehaye. The website provides a tool to send access and portability requests to data controllers. Personaldata.io has assisted in many high-profile access requests -- often by journalists -- such as those by Judith Duportail to Tinder, and by Carole Cadwalladr on the Facebook/Cambridge Analytica scandal. Paul-Olivier Dehaye himself has exercised his rights towards Facebook and has testified about the limited compliance as an expert witness to a UK parliamentary committee that is looking into the Cambridge Analytica/Facebook data misuse scandal.

Personaldata.io also runs a data wiki.[141] The goal of the wiki is to collectively build a database for mapping the personal data ecosystem. The ideal is to have information on organisations that process personal data, including the contact details of their DPO, the personal data that they collect, and the data flows between organisations. Personaldata.io also operates a forum for discussions about collective actions involving the right of access and expansion of the database.[142]

4.4. Selbstauskunft

Selbstauskunft.net is a Germany-based service through which so far over 1,150,000 data subject access requests have been sent.[143] A difference with other services like MyDataDoneRight or Access My Info is that the request letters are sent directly by the company behind selfstauskunft, by fax. Moreover the service is provided for free for up to three requests per person per year. A subscription costing €9.90 per year is available which allows to send more requests. There is also a blog connected to the service which has over a 100 posts running from 2010 to 2014.

The service also asks people to rate the responses they receive on a 1-5 scale, and also allows them to leave comments. Statistics of the scores that organizations receive can also be found on the website.

4.5. Data Rights Finder

Data Rights Finder by Open Rights Group (ORG) provides easily understandable information about companies' privacy policies and has contact information on 45 organizations and

139 Andrew Hilts and Christopher Parsons, 'Access My Info: An Application That Helps People Create Legal Requests for Their Personal Information', in The 15th Privacy Enhancing Technologies Symposium, Philadelphia, PA, 2015.

140 'PersonalData.IO', accessed 13 May 2020, https://wiki.personaldata.io/wiki/Main_Page.

141 'PersonalData.IO'.

142 'PersonalData.IO Forum', PersonalData.IO forum, accessed 13 May 2020, https://forum.personaldata.io/.

143 'Selbstauskunft.Net', accessed 13 May 2020, https://selbstauskunft.net/.

focuses on financial services industry.[144] Moreover, it provides templates for data subject rights as well as relevant contact information.

ORG is also using access requests in its campaign "Who do political parties think we are?"[145] In this campaign they invite citizens to file an access request with all the political parties that participate in the 2020 parliamentary elections and provide a tool for sending the requests.

144 'Data Rights Finder', accessed 13 May 2020, https://www.datarightsfinder.org.

145 Open RIghts Group, 'Who Do Political Parties Think We Are?'