Data Policies: Regulatory Approaches for Data-Driven Platforms in the UK and EU

IDRC project# 108339-003

Study for the larger collaborative project *Policy Frameworks for Digital Platforms - Moving from Openness to Inclusion*, coordinated by ITforChange, India

Author:

Dr Arne Hintz
Data Justice Lab
School of Journalism, Media and Culture
Cardiff University
UK

Final Technical Report

26 January 2019

Executive Summary

This Technical Report summarizes the findings and achievements of the research project *Data Policies: Regulatory Approaches for Data-driven Platforms in the UK and EU* which members of the Data Justice Lab at Cardiff University, UK, conducted between December 2017 and November 2018. The project contributed a specific study to a larger collaborative project, coordinated by ITforChange, entitled *Policy Frameworks for Digital Platforms - Moving from Openness to Inclusion.*

The study analysed trends and implications of current policy reform for data collection, analysis and sharing via platforms. In particular, it interrogated emerging regulatory frameworks that shape, constrain or advance citizens' control over data that concerns them and that affects their lives. It focused on policy change in the UK and EU, particularly the EU General Data Protection Regulation (GDPR) and the UK Investigatory Powers (IP) Act and Digital Economy (DE) Act, as a political and economic environment where rapid change in both platform and data policies is emerging.

The research methods for this study encompassed a) literature and document analysis regarding recent policy change, b) interviews with relevant stakeholders (government, industry, civil society), and c) expert workshops. The outputs generated by this project include a) a policy overview and b) a research report (both submitted to ITforChange as components of the broader project outcomes); c) presentation of results at international conferences (incl. so far, the European Communication Research and Education Association ECREA, Lugano, 1 November 2018); d) publication of research results in academic publications (incl. an article in the journal *Surveillance & Society* and a chapter in the book *Data Justice*, both currently under review).

The study found an emerging but incomplete and often contradictory regulatory environment for user data collection and analysis on/by platforms. On the one hand, there is growing recognition of the need to protect citizens' rights in an increasingly datafied society and to enhance citizens' control over data that affects them, as demonstrated by the new provisions of the GDPR. On the other hand, the collection and sharing of data, particularly by public authorities, is expanding and is being legalized and normalised through laws such as the IP Act and DE Act. Despite increased attention to data protection and the ethics of data uses, the risks of data collection and thus of pervasive monitoring of citizens through data generated on platforms persist.

The implications for platforms businesses of new data protection regulations are limited, so far. A sustained trend towards enhanced citizen control can, however, lead to change in the relations between platforms and users.

The Research Problem

With the proliferation of social media platforms, cloud services and the so-called 'sharing economy', our online interactions increasingly rely on a small number of concentrated businesses that provide (or limit) access to online services, regulate interactions between users, and make decisions on what content is fit to be published, shared, and found. The rapid emergence of platforms has led to a policy vacuum, and many of the activities and social, political and economic consequences of platforms have remained unregulated. This points to a need for policy development.

The collection, analysis and sharing of user data requires particular attention – in part, because they have significant implications for users and for state-business-citizen relations, and in part, because they affect the core business model of commercial platforms. Consumer, communication and service platforms collect and monetize a vast range of data, often without the knowledge of their users. Personal data as well as data derived from user activities on those platforms is systematically extracted, processed, and combined with additional datasets in order to create detailed profiles that are valuable to both the business sector and the state. Citizens are increasingly sorted, categorized and assessed according to this data and the profiles that are generated from it.

It is therefore pertinent to understand how data collection and analysis on platforms are regulated and whether – and, if so, how – this policy environment is changing. From a perspective of development, social justice and social change, it is particularly relevant to interrogate emerging regulatory frameworks that shape, constrain or advance citizens' control over data that concerns them and that affects their lives; to advance scholarly and public debate about these dynamics; and to investigate areas of potential intervention to address citizen needs and concerns.

The United Kingdom (UK) and the European Union (EU) offer a useful case study as they a) constitute a national and regional space where platforms play a significant role in social and economic life; b) have been the backdrop for prominent debates on data collection and analysis, from the Snowden revelations to the Cambridge Analytica / Facebook scandal; and c) have generated significant new laws and regulations that are likely to affect policy environment in other parts of the world. These include the following:

- UK Investigatory Powers (IP) Act 2016: a comprehensive legislation to combine the fragmented rules for state-based data collection and analysis under one law, addressing a wide range of surveillance practices – from bulk data collection to 'computer network exploitation' (i.e., hacking)
- UK Digital Economy (DE) Act 2017: regulates electronic communications infrastructure and services, requires further data collection by certain types of platforms, and facilitates data sharing between government departments
- EU General Data Protection Regulation (GDPR) 2018: limits the use and sharing of personal data by companies inside the EU as well as the export of data outside the EU; assigns citizens a wide set of rights to e.g., explanation of data processes, challenge outcomes of algorithmic decisions, and transfer their data to other platforms; strengthens consent rules; and requires impact assessments for potentially harmful data uses.

The original research goal was to analyse the effectiveness and consequences of these new rules in the immediate aftermath of their adoption. Specific questions addressed the agendas

that inform and underpin policy change, the responsiveness of policy processes to public concerns, regulatory responses to exclusions, inequalities and discriminations in the platform economy, gaps and inconsistencies in the current policy framework, and new or alternative approaches towards regulating the use of citizen data.

This goal was adapted slightly after the first stage of research – the literature and document analysis – and in response to other studies that already existed or were in the process of development. While useful analyses of the specific articles and provisions of these new rules were already being conducted by legal scholars, a broader perspective on the regulatory trends that emerged from these, across different laws and with a focus on citizen rights and social justice, was missing. This is where we believed the *Data Justice Lab* could make a significant and original contribution. The project design and overall project goals remained as planned, but a particular focus was placed on investigating the above-mentioned laws and regulations as *examples* for contemporary policy trends that affect the roles and rights of citizens in a datafied society.

Progress Towards Milestones

As this was a relatively limited study that fed into the larger project managed by ITforChange, the Grant Agreement only specified the Final Technical Report as milestone for the grantee (which is hereby submitted).

Further milestones agreed between the grantee and ITforChange included

- Participation in project workshop, Mumbai, June 2018 (I participated and presented preliminary research outcomes)
- A policy overview (draft submitted in September 2018, final version in October 2018)
- Research Report (draft submitted in December 2018, final version to be submitted in February 2019).

Research progress was slightly delayed due to unforeseen requirements of other research projects that the Data Justice Lab was conducting, but research was completed as planned.

Synthesis of Research Results and Development Outcomes

The study identified two opposing trends in data policy: an increase in data collection by both commercial and state actors, on the one hand, and a growing recognition of citizens' rights and control over data, on the other.

The momentum for citizen control emerged as part of persistent critiques of platform power and data extraction, was fuelled by data-related scandals, such as the Cambridge Analytica case and the Snowden revelations, and was underpinned by sustained efforts of digital rights campaigners. Its main policy expression has been the GDPR which has introduced a range of regulations that both enhance citizens' active role in the datafied society and protect them from data-related harms. These include, among others, the right of access to personal data and to data portability, the right to explanation for citizens to understand how their data is used, stricter requirements for user consent and purpose limitation of data, and restrictions to profiling and

automated decision-making. The need for data autonomy has reached the UK policy debate and there is some political will to address citizen concerns regarding data extraction practices of platforms (as, e.g., the UK Digital Charter and Data Protection Act, both from 2018, demonstrate).

However these provisions provide a starting-point, at best, for strengthening citizen rights. Several of the more specific rules have severe limitations and loopholes; the onus is largely placed on the 'informed' user, for example by maintaining the widely criticised concept of 'user consent'; and the focus remains on 'personal data', excluding the increasingly relevant range of inferred and derived data based on much wider set of online behaviour, transactional data, health data, etc. Moreover, data collection and data sharing are expanding, allowed and mandated by laws such as the IP Act and the DE Act. In particular, those policies require platforms to make more of their data available to public authorities. As our interviews have shown, there is no appetite among policymakers for restrictions to the collection of data in the name of citizen control. In their view, sparsely restricted collection of data should be balanced by rules constraining its use, such as data ethics guidelines. Civil society members disagreed and pointed to the continued risks emerging from data collection. Overall, the debate on ethical data use and the protections by the GDPR may turn attention away from questions of data collection, without addressing its risks and concerns. Data ethics and data protection may thus have the (intended or unintended) consequence of legitimising and advancing data collection.

The research also pointed to conceptual limitations of the policy debate. The focus on 'personal' data and on individual approaches to handle one's data neglects the collective nature of data which typically denotes a relation to others – as demonstrated in social networks as well as the data-based categorizations, rankings and 'risk scores' that are at the core of contemporary forms of algorithmic governance. Innovative approaches to address the collective, rather than individual, dimension of data have emerged, for example, through the concept of indigenous data sovereignty. Yet such concepts remain underdeveloped in a European policy context. Data localisation, a strategy advanced by several governments and civil society organisations in the Global South, remains unattractive to all stakeholders interviewed in this study due to suspicions that this may merely advance government access to data.

The interviews, in particular, demonstrated competing policy goals and value systems between different stakeholder groups. Dominant sectors of the state have successfully established 'security' (or rather, a specific understanding of national security) as a prominent benchmark while business interests have used 'innovation' as the frame for guiding data policy and, specifically, for allowing data uses with limited restrictions. In this context, the protection of citizens and the enhancement of their control over data that concerns them have to assert their place (and, according to government representatives, be 'balanced') against these goals.

Overall, as this study shows, the discourse of increased citizen control and empowerment is growing and is gaining traction in policy debate. There is an emerging understanding that the policy environment for the data-related activities of platforms (and, by extension, for data collection and analysis more broadly) is insufficient. However the actual implementation of citizen control, so far, is subject to significant limitations based on narrow definitions of such control and an expansion, rather than reduction, of data collection and sharing, particularly by state agencies. Citizens are gaining new capabilities due to the GDPR but are also subject to increased monitoring, and the data they have access to and power over remains a limited section of the wider range of data that is now used in the private and public sector. We may be a long way off actual citizen control over data, but we are witnessing openings and new avenues towards that goal.

The study highlighted these complex interactions and observed, as well as criticised, a new data policy paradigm in the making. This will, first of all, inform the broader collaborative project, but it may also stand on its own in contributing to scholarly debates (particularly, in the field of critical data studies) and policy practice. To that end, we are planning a presentation at the conference 'Data for Policy' in London in June. As the study has shown, the policy environment for data is in constant development, which opens possibilities for impactful interventions into the debate.

Methods

The study combined desk research, expert interviews, and expert workshops. As a first step we conducted a review of both academic and public literature on the policies that formed the core of the analysis – IP Act, DE Act and GDPR. We reviewed journal articles, blog entries and other literature that emerged in the immediate aftermath of or, in the case of GDPR, before the adoption of the new policies. This review was conducted between January and March 2018.

This research was complemented by meetings and workshops that brought together different stakeholders and affected groups. In particular, we held a workshop as part of the conference *Data Justice* at Cardiff University, 21-22 May 2018, to review current policy frameworks, identify gaps and shortcomings, and explore proposals for policy reform.

Finally, we conducted semi-structured interviews with members of different stakeholder communities, with the goal of exploring different perspectives on the specific laws and regulations as well as on key themes that emerged, and to investigate broader regulatory trends. The interviews took place between August and October 2018. They are listed in the table below. All interviewees are policy officers or policy directors in their organisations and concerned with questions closely related to those addressed in this research project; 5 interviewees were male and 2 female; and all are based in the UK.

Interviewee #	Stakeholder group	Organisation
Interviewee 1	Government	UK Department for Digital, Culture, Media and Sport
Interviewee 2	Government	UK Department for Business, Energy and Industrial Strategy
Interviewee 3	Business	Internet Service Providers Association (ISPA)
Interviewee 4	Business	techUK (Business association)
Interviewee 5	Civil Society	Open Rights Group
Interviewee 6	Civil Society	doteveryone
Interviewee 7	Civil Society	Privacy International

Project Outputs

The outputs generated by this project include the following:

a) Input to the broader project 'Policy frameworks for digital platforms': a policy overview document and a research report. The policy overview has been concluded, the research report has been submitted in draft form and will be revised and completed in February 2019.
b) Academic publications: To date, one article has been submitted to, and accepted by, the open access journal *Surveillance & Society*, as part of a special issue on platforms. At least one further article will be submitted (to a different journal in the discipline of media and communication studies). The proposed co-authored book *Data Justice* (to be published by Sage, 2020) will have a chapter on Data Policies based on this study.
c) Presentation of results at international conferences: To date, one presentation on the findings of this study was held at the annual conference of the European Communication Research and Education Association (ECREA), Lugano, 1 November 2018. A further presentation has been proposed for the conference *Data for Policy*, London, 11/12 June 2019.

Problems and Challenges

As this has been a relatively small project, we have not encountered any major issues. There have been a few delays to the completion of the project, partly due to internal workload reasons (as we were conducting this project in parallel with other projects and full-time academic jobs), and partly because of scheduling issues with our preferred interviewees. However this has not led to any significant changes to project design or outputs.

We did not encounter ethical challenges beyond the general sensitivity of the research topic. Our interviewees were willing to talk with us and agreed with the proposed arrangements regarding the anonymity of sources.

Administrative Reflections and Recommendations

This study provided input for a larger collaborative project, and our main interactions regarding milestones and outputs occurred with ITforChange. This has worked well, our working relationship with ITforChange has been positive, and it seems like a useful model for conducting a broader project like this. Whether, in this case, separate reports for the funder and for the project leader are necessary may be debatable but may depend on funding guidelines. Overall, this has been a positive experience.