Exercising democratic rights under surveillance regimes[1]

Executive Summary[2]

Dr Xavier L'Hoiry & Professor Clive Norris

In the context of surveillance and democracy, the principles of consent, subject access and accountability are at the heart of the relationship between the citizen and the information gatherers. The individual data subject has the right to at least know what data is being collected about them and by whom, how it is being processed and to whom it is disclosed. Furthermore, they have rights to inspect the data, to ensure that it is accurate and to complain if they so wish to an independent supervisory authority who can investigate on their behalf.

The second of these three principles, one's right of access to personal data, is a central feature of European data protection regulatory framework and in particular of the European Data Protection Directive 95/46/EC. It is, arguably, the most important of the so called ARCO data protection rights (access, rectification, cancellation, opposition) because, if one cannot discover what is held about oneself, it is not possible to exercise the remainder of these rights.

Our research found, however, that the spirit of the European Data Protection Directive has frequently been undermined as it has been transposed into national legal frameworks, and then further undermined by the evolving national case law. Citizens, in their role of data subjects, encounter a wide range of legitimate but not always convincing and straightforward restrictions in their attempts to exercise their rights. These legal restrictions are further undermined by illegitimate actions enacted through a series of discourses of denial practiced by data controllers or their representatives.

The research was conducted in three parts. The first part involved a comparative analysis of European and national legal frameworks in the areas of data protection and, specifically, subject access rights. The second part saw researchers undertake empirical work in attempts to locate data controllers, their contact information and key content regarding data protection and subject access rights. The third part continued this empirical work and tasked researchers with submitting subject access requests, in relation to their own personal data, to a range of data controllers to assess this process as well as the responses received from these organisations. As such, this Deliverable is made up of country reports written by researchers in the ten participating institutions. These country reports are available in the appendix section of the Deliverable and offer in-depth analyses of exercising informational rights in country-specific contexts.

---

[1] This version of the report is a draft. It is yet to be formally approved by the European Commission.

[2] The following partners were involved in the research and the data presented here is the result of their fieldwork: Professor Clive Norris (University of Sheffield, UK); Dr Xavier L'Hoiry (University of Sheffield, UK); Antonella Galetta (Vrije Universitiet Brussel, Belgium); Professor Paul de Hert (Vrije Universitiet Brussel, Belgium); Dr Ivan Szekely (Eotvos Karoly Institute, Hungary); Beatrix Vissy (Eotvos Karoly Institute, Hungary); Dr Rocco Bellanova (Peace Research Institute Oslo, Norway); Professor J. Peter Burgess (Peace Research Institute Oslo, Norway); Maral Mirshahi (Peace Research Institute Oslo, Norway); Stine Bergensen (Peace Research Institute Oslo, Norway); Marit Moe-Pryce (Peace Research Institute Oslo, Norway); Jaro Sterbik-Lamina (Institute of Technology Assessment, Austria); Stefan Birngruber (Institute of Technology Assessment, Austria); (Dr Chiara Fonio (Universita Cattolica del Sacro Cuore, Italy); Alessia Ceresa (Universita Cattolica del Sacro Cuore, Italy); Professor Marco Lombardi (Universita Cattolica del Sacro Cuore, Italy); Dr Gemma Galdon Clavell (Universitat de Barcelona); Liliana Arroyo Moliner (Universitat de Barcelona); Dr Erik Lastic (Univerzita Komenskeho v Bratislave, Slovakia); Roger von Laufenberg (Institut fur Rechts und Krimialsoziologie, Austria); Professor Nils Zurawski (Universitat Hamburg, Germany)

Legal Frameworks

Data subjects are inherently disadvantaged before they can even begin the process of submitting a subject access request. This is in part because the implementation of the EU Data Protection Directive 95/46/EC has been uneven across EU Member States and, together with the development of case law, many European countries have interpreted key provisions of the European law in a narrow way.

As a consequence, European citizens living in different countries are subject to very different regimes in relation to:

- legally defined response time obligations on data controllers;
- requirements upon data controllers to appoint Data Protection Officers;
- the costs of making a subject access request;
- the complaints and redress mechanisms available to data subjects with their national Data Protection Authorities.

This means that, not only is there considerable differences at the European level, but that an access request emanating from one country, but submitted to another, may be subject to completely different procedures. This inconsistency is particularly true of provisions in relation to the concept of 'motivated requests' in the area of CCTV, (Belgium and Luxembourg) which demand that data subjects legitimise their requests with a justified reason accompanying the submission of the request itself. In such cases, it seems that exercising one's rights as set out in the European Data Directive is not a justified reason in and of itself, and often leaves the data subject at the mercy of the data controller's discretion to determine what constitutes a legitimate reason.

Locating the Data Controller

The right of access is exercised by submitting an access request to a given data controller but, before this can begin, one must locate the data controller itself. This phase of the empirical work was conducted as follows:

- The research was conducted across 10 European countries[3] and examined 327 individual sites in which one's personal data was routinely collected and stored.
- The research sites were chosen based on a consideration of the socio-economic domains in which citizens encounter surveillance on a systematic basis. These domains were health, transport, employment, education, finance, leisure, communication, consumerism, civic engagement, and security and criminal justice.
- Researchers attempted to locate data controllers and their contact details in a variety of ways including by telephoning them, by attending sites in person and by accessing organisations' online content.

The research sought to determine the ease and/or difficulty of locating data controllers, given the centrality of this process as the natural pre-condition of citizens being able to exercise informational self-determination.

The research found that, in a significant minority (20%) of cases, it was simply not possible to locate a data controller. This immediately restricts citizens' ability to exercise their right of

[3] The research was carried out in the following countries: Austria, Belgium, Germany, Hungary, Italy, Luxemburg, Norway, Slovakia, Spain and the UK.

access because insufficient information is given regarding to whom one should send access requests. Where data controllers could be located, the quality of information concerning the process of making an access request varies enormously from country to country and in different sectors, both public and private. In the best cases, information was thorough and followed legislative guidelines closely, providing citizens with an unambiguous pathway to exercise their right of access. In the worst cases information was very basic, often failing to explain how to make an access request or indeed what an access request actually is. Information was often confusing and incomplete, consequently obliging the citizen to pro-actively seek out clarification before being in a position to submit a request.

The most reliable, efficient and frequently used way of locating data controllers turned out to be on-line. In nearly two thirds (63%) of all cases on-line searching provided the relevant contact details, and this was achieved in less than five minutes over half (61%) of the time.

Attempts to locate data controllers using alternative methods generally did not fare well. In the majority of cases, when contacting organisations by telephone, members of staff lacked knowledge and expertise concerning subject access requests. As a result, answers were often incorrect, confusing and contradictory to their own organisations' stated policies.

When it was possible to locate the data controller via telephone, this took over 6 minutes, sometimes on premium rate lines, in over half (54%) of all cases. And even then, the quality of information provided via telephone was rated as 'good' in only 34% of cases.

In the case of CCTV, where we attended the sites in person:

- nearly 1 in 5 sites (18%) did not display any CCTV signage;
- where signage was present, in over four out of ten cases (43%) it was rated as being 'poor' in terms of its visibility and content;
- only one third (32.5%) of CCTV signage identified the CCTV system operator or the data controller.

By failing to display appropriate signage at CCTV sites, one fifth of organisations effectively employed 'illegal' practices. The expertise of members of staff when approached in person was often lacking and they frequently reacted to queries with suspicion and scepticism, questioning why one would wish to access their personal data. Thus, even where researchers were merely trying to find the contact details of the data controller, they were forced to justify why they sought to exercise their democratic rights, and even then they were frequently denied.

Submitting Access Requests

When it is possible to locate the data controller, the process of then submitting an access request can be problematic with data controllers employing a range of discourses of denial which restrict or completely deny data subjects the ability to exercise their informational rights.

- Subject access requests were sent from 10 European countries to 184 individual organisations sampled from the first part of the empirical phase of the research.
- This sample set included both public and private sector organisations as well as a number of key multinational organisations which routinely collect large amounts of data.

- The requests were made for a range of data including information held on paper and digital records as well as CCTV footage.
- Requests made three key demands of data controllers: disclosure of personal data; disclosure of third parties with whom data had been shared and disclosure of whether (and if so how) data had been subject to automated decision making processes.

The research found that obtaining a satisfactory response concerning all aspects of the requests was a relatively rare occurrence.

- Four out-of ten requests (43%) did not result in personal data being disclosed or data subjects receiving a legitimate reason for the failure to disclose their personal data.
- In over half of all cases (56%), no adequate or legally compliant response was received concerning third party data sharing.
- In over two-thirds of cases (71%) automated decision making processes were either not addressed or not addressed in a legally compliant manner.

Even taking account of those cases in which successful outcomes were achieved, the process of submitting an access request was often fraught, confusing and time-consuming.

- Holding/acknowledgement letters were received in only a third (34%) of cases, which meant that data subjects had no idea as to whether the requests were being dealt with or simply ignored.

- Even where data subjects received their personal data, the disclosure of this data was incomplete and additional data was still outstanding. This occurred in one third of cases (31%) and required researchers to pursue data controllers for more information as the first disclosure was incomplete.

There were noted variations in how different types of organisations responded to requests. In general, public sector organisations performed less badly than those in the private sector, with only 43% engaging in restrictive practices compared with 62% in the private sector. Requests for CCTV footage were particularly problematic, with seven out of ten requests for CCTV footage being met by restrictive practices from data controllers or their representative. While loyalty card scheme operators were generally facilitative in disclosing personal data (86% of cases), they did not perform as strongly in providing information about automated decision making processes (only 50% of cases). Meanwhile, requests made to banks did not yield much information about third party data sharing (only 30% of responses disclosed this).

In assessing both the process of submitting access requests as well as the content of the responses received from data controllers, the research found a range of restrictive practices employed.

- Data controllers frequently render themselves 'invisible' to data subjects using a variety of practices, ranging from the absence of CCTV signage identifying who is operating the cameras to flatly refusing to respond to access requests at all. In 12 cases, requests were met with complete silence. In a further 17 cases, although preliminary communications were entered into, any subsequent correspondence elicited no response. In total, therefore, in the end, one in six cases (15%) of all cases was met with silence.
- Many organisations did not have clear and formal administrative procedures in place to receive and respond to subject access requests. These bureaucratic failures led to

considerable delays and confusion for data subjects in the way that their requests were processed. This included the inability (or unwillingness) of data controllers to respond to requests in any language other than English despite receiving requests in other languages.

- Data controllers often responded to requests only after long and excessive delays. This at times had a direct impact on the availability of the data requested (e.g.: the deletion of CCTV footage). It also meant that data controllers were in breach of their legal obligations to respond to requests within nationally specified time frames.
- Some data controllers, particularly multinational corporations, offered only fixed and pre-determined mechanisms for data subjects to submit requests. These mechanisms did not allow for specific queries to be addressed and took an extremely narrow and, in the context of European law, invalid interpretation of what type of data citizens are entitled to request.
- In many cases, data controllers refused to fulfil requests by invoking legal provisions incorrectly. This belied a lack of knowledge and expertise on behalf of data controllers and their representatives because data subjects were erroneously advised that they had no legal entitlement to exercise their rights.

Achieving a successful outcome when submitting an access request is possible and we came across a significant minority of cases, for instance in Germany and the UK, where requests were dealt with courtesy, diligence and efficiency. However, the burden of achieving a successful outcome lies heavily with the data subject and many organisations in this research did little to lift this burden away from the citizen: members of staff repeatedly reacted with surprise and puzzlement to our requests, explaining that they had never before received such queries. A vicious circle therefore emerges, where organisations fail to inform citizens of their rights or how to exercise them. As a result, for those citizens who have little or no prior knowledge about privacy and data protection issues, the right of access is either unknown, denied or inaccessible. Then due to the lack of subject access related queries received from the public, organisations fail to inform/train their staff in matters of privacy and data protection, and have little motivation to do so.

The empirical results of the research demonstrated significant disparities in the ways requests were processed from one country to another. The research shows that this is partly due to the willingness of Data Protection Authorities in some countries to support citizens when they exercise their informational rights. This, coupled with the absence of the need for data subjects to provide a justified motivation for their requests, meant that submitting such requests was generally a smooth process in these countries. In contrast, in Italy and Spain, the researchers encountered a plethora of restrictive practices ranging from the identification of data controllers, the ways in which their requests were processed and the difficulty of submiting complaints to DPAs when disputes arose.[4]

The results of the research have led to a wide number of broad and general policy recommendations. Some of the key points to emerge are the following[5]:

[4] The individual country reports located at Appendix 1 in this deliverable provide comprehensive analyses of the experiences of data subjects in this research in these countries.

[5] The key policy recommendations outlined here are a mere snapshot of the full spectrum of the policy implications and recommendations which have emerged from the research. The full outline of policy recommendations is available in the Policy Implications and Recommendations section of the deliverable.

- Data controllers should take steps to render themselves more ‘visible’ and simplify the access request process for data subjects by implementing recognised procedures to process access requests.
- Data controllers should provide data subjects with clear and intelligible information about which personal data they process and how data access requests may be introduced.
- There should be no motivation required when submitting an access request other than the wish to exercise one’s democratic rights, notably the right to the protection of personal data.
- If data controllers invoke legal exemptions when refusing an access request, they should demonstrate upon which exemptions they are relying.
- Data Protection Authorities should provide templates and guidance for data subjects and data controllers to use when citizens are seeking to exercise their informational rights.
- Data Protection Authorities should also provide an unambiguous and free redress mechanism for data subjects to bring complaints.
- Civil society organisations should be encouraged to promote access and other informational rights.

The myriad of restrictive practices evidenced in this research means that data subjects have to work extremely hard to exercise their rights. They must show persistence, confidence and resilience in the face of a series of discourses of denial during which their access requests may be regarded as illegitimate, severely delayed or simply ignored altogether. And even then, they are only likely to have successfully exercised their rights fifty-percent of the time.