INCREASING RESILIENCE IN SURVEILLANCE SOCIETIES (IRISS)

COORDINATED BY DR. REINHARD KREISSL
IRKS INSTITUT FÜR RECHTS- UND KRIMINALSOZIOLOGIE
WEIN, AUSTRIA

DELIVERABLE D5: EXERCISING DEMOCRATIC RIGHTS UNDER SURVEILLANCE REGIMES

LED BY PROFESSOR CLIVE NORRIS AND DR XAVIER L'HOIRY
DEPARTMENT OF SOCIOLOGICAL STUDIES
UNIVERSITY OF SHEFFIELD, UK

UNITED KINGDOM COUNTRY REPORTS

UNIVERSITY OF SHEFFIELD, UK

PARTS:

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS IN THE UNITED KINDGOM – DR XAVIER L'HOIRY & PROFESSOR CLIVE NORRIS

LOCATING THE DATA CONTROLLER IN THE UNITED KINGDOM – DR XAVIER L'HOIRY & PROFESSOR CLIVE NORRIS

SUBMITTING ACCESS REQUESTS IN THE UNITED KINGDOM – DR XAVIER L'HOIRY & PROFESSOR CLIVE NORRIS

MAPPING THE LEGAL AND ADMINISTRATIVE FRAMEWORKS OF ACCESS RIGHTS IN THE UNITED KINGDOM

Application (primary and secondary legislation) and interpretation (case law) of data protection principles

In the UK, the Data Protection Act (DPA) 1998[1] covers the majority of privacy and subject access rights.[2] The 1998 Act was passed to replace its 1984 predecessor following concerns that previous definitions and criteria did not reflect the wide-ranging intentions of the Directive and were therefore potentially incompatible. Section 1(1) of the DPA 1998 defines personal data as:

> "...data which relate to a living individual who can be identified –
> (a) From those data or
> (b) those data and other information which is in the possession of, or likely to come in the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of that individual".[3]

'Data controllers' meanwhile, are defined thus:

> "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed".[4]

The Act goes on to define 'processing' as:

> "obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data".[5]

A 'relevant filing system' under which data is stored is described as:

> "any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible".[6]

[1] Data Protection Act 1998, available online at http://www.legislation.gov.uk/ukpga/1998/29/contents
[2] The Data Protection Act 1998 should not be confused with the Freedom of Information Act 2000 which concerns itself mainly with the legal right of citizens to request publicly available information (*not* personal data) from public bodies by way of making a request known in the UK as a freedom of information request. This process is a generally well-known right and is frequently exercised by citizens. It has gained prominence via various media coverage and through activist websites such as www.whatdotheyknow.com which provides templates and guidance for the purposes of making requests and publishes the responses of public authorities.
[3] (S.1(1)(a)(b) DPA, 1998)
[4] (S. 1(1) DPA, 1998)
[5] (S. 1(1) DPA, 1998)
[6] (S. 1(1) DPA, 1998)

Finally, 'processing' is outlined as:

> "obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data".[7]

Section 7 of the DPA 1998 is concerned specifically with the right of access to personal data. The Act prescribes that requests must be made in writing (Article 7(2) DPA, 1998) and data controllers must respond within 40 days (S. 7(10) DPA, 1998). Reflecting the terms of the Directive, Section 7 of the DPA requires data controllers to inform individuals when controllers process personal data (S. 7(1)(a) DPA, 1998) and to present this to subjects upon request in an intelligible form (S. 7(1)(c) DPA, 1998).

Exemptions are listed in Part IV of the DPA 1998 and broadly reflect those outlined in the Directive. Sections 28 to 34 prescribe that numerous circumstances exist exempting data controllers from disclosing personal data and these include, most pertinently, national security, crime and taxation, regulatory activity and data used as part of legal proceedings. These are further explored in Section 3 below.

Application (primary and secondary legislation) and interpretation (case law) of the right of access to data

Durant v Financial Service Authority

The stand-out case concerning subject access rights in the UK is *Durant v Financial Services Authority* (2003) which was heard in the Court of Appeal. Briefly, Durant was in dispute with Barclays Bank and sought the help of the Financial Services Authority (FSA) in 2000. The following year, the FSA concluded its investigation but refused Durant's request to disclose details of the investigation due to confidentiality requirements as prescribed in UK banking law. Under Section 7 of the DPA, Durant sought disclosure of personal data processed by FSA in the course of their investigations. Specifically, Durant requested the records the FSA had obtained from Barclays Bank in order to make their decision. These included a wide range of financial documents in which Durant featured in varying degrees of prominence. Moreover, he requested these records in both electronic and manual form. The FSA responded by releasing redacted electronic records and refusing to release any manual data. Indeed, the FSA argued that not only did the records fail to meet the definition of 'personal data' (even though Durant was named and featured in the records), they also failed to meet the definition of 'data' as they were not stored in a 'relevant filing system'.[8]

Personal data

Following unsuccessful challenges by Durant at lower levels, the case was heard in the Court of Appeal and centred upon the definition of 'personal data' as the FSA argued that the data requested did not fulfil this definition. The court ruled in favour of the FSA, finding that the

[7] (S. 1(1) DPA, 1998)
[8] Jagessar, U. and Sedgwick, V. (2005) 'When is personal data not "personal data" – The impact of Durant v FSA', *Computer Law and Security Report*, 21(6): 505-511

information requested by Durant did not constitute personal data and in doing so, the court took a narrow interpretation of the term 'personal data'.

In delivering this judgement, the court explained that a narrow definition was faithful to the Directive's intentions and that Section 7 of the DPA was never intended to act as an "automatic key for information, nor to allow access to any and all documents mentioning the data subject's name, nor, importantly, any and all which may be retrieved by putting the subject's name into a search engine".[9] Instead, Section 7 intended to safeguard the privacy of individuals by enabling them to check what information data controllers held about them and that data controllers were processing such data lawfully. The judgement advised that whether any given information amounted to 'personal data' depended on where it fell in a 'continuum of relevance and proximity' to the subject. In order to clarify the meaning of 'personal data', the court provided two examples as guidance in this matter:

> "The first is whether the information is biographical in a significant sense, that is, going beyond the recording of the (individual's) involvement in a matter or an event that has no personal connotations, a life event in respect of which his privacy could not be said to be compromised.
>
> The second is one of focus. The information should have the (individual) as its focus rather than some other person with whom he may have been involved or some transaction or event in which he may have figured or have had an interest... In short, it is information that affects his privacy, whether in his personal or family life, business or professional capacity."[10]

As such, 'merely mentioning an individual's name in records was not necessarily enough'.[11] In the context of the case, the court found that a great portion of the information sought by Durant related in fact to Barclays Bank and FSA rather than Durant personally and as such did not constitute personal data according to their interpretation. They found in fact that Durant was 'misguided'[12] in seeking the information in this matter and that he had attempted to utilise Section 7 of the DPA to obtain data about a third party (Barclays Bank in this case).

Relevant filing system

Although ultimately inconsequential to the case given that Durant had failed to satisfy the personal data criteria, the court also provided clarification regarding the meaning of a data controller's 'relevant filing system'. The court here again interpreted this in favour of data controllers and the 'emphasis was on the need to avoid a disproportionate burden falling in data controllers'.[13] A 'relevant filing system', where not computerised, would need to resemble the efficiency, accessibility and sophistication of a computerised system, allowing a data controller ready access to requested information. As Jagessar and Sedgwick (2005) explain:

[9] Edwards, L. (2004) 'Taking the "personal" out of personal data: Durant v FSA and its impact on the legal regulation of CCTV', *Script-ed*, 1(2): 342-349, at page 343
[10] *Durant v Financial Services Authority* [2003] EWCA Civ 1746, supra n 3, para 28
[11] Wotherspoon, K. (2003) 'Access Denied – Court of Appeal rules on subject access requests', *Privacy Laws & Business*, 14: 1-3, at page 1
[12] *Durant v FSA*, op. cit. (2003) supra n. 3, para 31
[13] Wotherspoon, K. op. cit. (2003) p. 3

> "If a person has to 'leaf through files, possibly at great length and cost (remembering that a data controller can only require an individual to pay up to £10 in relation to his access request), to see whether it or they contain information relating to the person requesting information... (this would) bear no resemblance to a computerised search and therefore would not qualify as a 'relevant filing system'".[14]

Moreover, it would not be enough for files to be organised simply by name and/or date as the judgement outlined:

> "The documents are not organised in such a way that would enable one to isolate particular aspects of the information, save that it is all under the name Durant. It is in the file just by date order. It follows again that this does not in my judgment satisfy the requirement of structuring anticipated by the statutory provision".[15]

In the case of *Durant v FSA,* the court found that the data requested was not held in a relevant filing system by FSA and therefore this criterion was also unfulfilled.[16]

Other case law

The judgement in *Durant* was reinforced in subsequent case law. In *Johnson v Medical Defence Union* (2007), Johnson was a consultant orthopaedic surgeon whose professional indemnity insurance as part of membership to the Medical Defence Union (MDU) was not renewed as per the absolute discretion of the MDU. In response, Johnson sought all personal data from MDU and submitted a Section 7 request. MDU provided some documents but believing there to be other information not disclosed, Johnson undertook legal proceedings against MDU. The specific points of consideration in this case concerned not only the interpretation of 'data' but more pertinently the meaning of 'processing' according to the Act since some of the information sought by Johnson had been stored electronically by MDU and subsequently destroyed as per standard protocols. Johnson argued that "the information had been recorded with the intention that it is processed'[17] and 'recorded in a relevant filing system"[18] and as a result fulfilled the definitional requirements of the DPA. The Court ruled in favour of MDU and found that "data controllers can only be required to search through data which they have at the time of receipt of the access request".[19] This finding further narrowed the interpretation of the DPA and placed a lesser burden onto data controllers in responding to subject access requests. This finding was upheld on appeal in 2007.

In *Smith v Lloyds TSB Bank plc* (2005), Smith had been in long-running litigation with Lloyds TSB and sought to obtain personal data in order to strengthen this litigation. In this case, the court considered the meaning of a 'relevant filing system' as well as what constitutes 'personal data'. The data sought by Smith had at one time been stored electronically but at the time of the subject access request was stored in hard copy bundles kept in boxes. The court found that despite the data having previously been stored

[14] Jagessar, U. and Sedgwick, V. op. cit. (2005) p. 507
[15] *Durant v FSA*, loc. cit. (2003) supra n. 3, para 35
[16] *Durant v FSA*, loc. cit. (2003) supra n. 3, para 46
[17] As per S. 1(1)(b) DPA, 1998
[18] As per (S. 1(1)(c)) DPA, 1998
[19] Jagessar, U. and Sedgwick, V. op. cit. (2005) p. 508.

electronically, the manual storage did not satisfy the meaning of 'relevant filing system' as proposed in *Durant* (i.e.: someone would be required to leaf through the files to find the relevant data) and as such Lloyds TSB were under no obligation to provide the data. Moreover, the court found that the data sought by Smith was not 'personal data' insofar as it related to business dealings between Lloyds TSB and companies of which Smith was a managing director. As such, although Smith's name appeared in the information, this was not biographical and the nature of the data did not pertain to Smith's privacy.

Finally, in *Ezsias v Welsh Ministers* (2007), the High Court further appeared to ease the burden upon data controllers. Ezsias was involved in legal proceedings with his former employer, North Glamorgan NHS Trust. He claimed that the defendants had not complied with their obligations under the Act by firstly failing to provide the data requested within 40 days and secondly by failing to provide all the data to which he was entitled. While the court upheld that the data had not been provided within 40 days, the defendants were deemed to have acted "reasonably and proportionately",[20] as per the DPA 1998, in their searches for the claimant's data despite the fact that they had not disclosed the entirety of his requested documentation. His request was deemed to have been too wide-ranging as he had asked for *all* documents in the possession of the defendants which related to him. As such, the court effectively found that responding to Ezsias's request in full would have involved a disproportionate effort on behalf of the data controller, North Glamorgan NHS Trust. Despite finding that the defendants had indeed failed to comply within 40 days, the court found that Ezsias had not suffered any damage by this failure to comply. Indeed, in the context of the case, the judgement found the defendants' failure to comply with the 40 day time limit to be "of little importance".[21]

National exceptions to the EU Data Protection Directive and to the right of access to data

Part IV of the DPA 1998 lists a number of exemptions to the right of access to personal data. The most common of these exemptions are as follows:

- Circumstances in which disclosure is likely to prejudice national security. (S. 28, DPA 1998)
- Circumstances in which disclosure is likely to prejudice the prevention of detection of crime. (S. 29, DPA 1998)
- Circumstances in which disclosure is likely to prejudice the capture or prosecution of offenders. (S. 29, DPA 1998)
- Circumstances in which disclosure is likely to prejudice the assessment or collection of tax or duty. (S. 29, DPA 1998)
- Social work records if disclosure is likely to prejudice the carrying out of social work by causing serious harm to the physical or mental health of the requester. (S. 30, DPA 1998)
- Health records – as per the social work provisions above. Health records can also be exempt if disclosure is likely to prejudice other individuals mentioned in the documentation. (S. 30, DPA, 1998)
- Educational documents – a document may be exempt if it does not fall within the educational record of the child. The Information Commissioner's Office (hereinafter

[20] *Ezsias v Welsh Ministers* [2007] All ER (D) 65 (Dec) para 158.
[21] *Ezsias v Welsh Ministers*, ibid. (2007) para 106.

ICO), the data protection authority in the UK, provides the example of a teacher's note on a pupil solely for their own use or information about the pupil provided by the parent of another child (ICO, 2012). (S. 30, DPA 1998)

- Documents pertaining to regulatory activity being carried out. (S. 31, DPA 1998)

Other exemptions in the Act include:

- Journalism, literature and art (S. 32, DPA 1998).
- Research, history and statistics (S. 33, DPA 1998)
- Manual data held by public authorities (S. 33A, DPA 1998)
- Information available to the public by or under enactment (S. 34, DPA 1998)
- Disclosures required by law or made under legal proceedings (S. 35, DPA 1998)
- Parliamentary privilege (S. 35A, DPA 1998)
- Domestic purposes (S. 36, DPA 1998)
- Miscellaneous Exemptions (S. 37, DPA 1998)
    - This relates in particular to the following: human fertilisation and embryology: information about the provision of treatment services, the keeping or use of gametes or embryos and where identifiable individuals were born in the consequence of treatment services. Also includes adoptions records and reports; statement of child's special educational needs; parental order records and reports. (Parts I & II of The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000)
- Powers to make further exemptions by order (S. 38, DPA 1998).

A further exemption applies in the case of disclosing personal data which include data on a third party (S.7(4)). The ICO has provided some guidance in this matter and explains that data controllers do not need to provide information if it involves third party data unless:

- the third party has given consent
- it is reasonable in all the circumstances to comply with the request without the third party's consent.[22]

The ICO explains that data controllers are expected to undertake a balancing analysis of whether the subject access request supersedes the third party's rights in respect of their personal data.[23] Data controllers are urged to avoid blanket policies in these circumstances and consider the merits of each request on a case-by-case basis. In some circumstances, a duty of confidentiality will arise which will inform the data controller's decision – the ICO uses the example of a doctor-patient relationship. In cases where the data controllers upholds the third party's right, the ICO advises data controllers to take steps to still disclose as much data as possible to the requester – this may involve providing redacted documents. Data controllers must be able to justify their decision to refuse disclosure of information due to the existence of third party data.[24]

Compatibility of national legislation with Directive 95/46/EC

Post-Durant – Impact and criticism

[22] Information Commissioner's Office, op. cit.. (2012) p. 32.
[23] Information Commissioner's Office, ibid. (2012).
[24] Information Commissioner's Office, ibid. (2012).

The judgement in *Durant v FSA* has received considerable criticism, chiefly for the narrow interpretation it gave to 'personal data' and the potential impact of such a reading of the intentions of the Directive and the DPA. It is worth noting that the narrow interpretation in *Durant* is directly juxtaposed to the subsequent opinion expressed by the Article 29 Working Party No. 136 regarding the concept of personal data.[25] Emphasising the centrality of the definition of 'personal data' in the concept of data protection, Chalton, explains that "to define personal data restrictively is to limit the scope of data protection at large, both in respect of automatically processed data and in respect of data held in manual files, and so is of key importance".[26] Chalton further asserts that in *Durant*, the Court of Appeal effectively reduced the rights of individuals and that 'there may now be uncertainty about the interpretation of the term 'personal data' by other Member States' national courts, with consequent risks of disharmony and resulting effects on flows of personal data within the European Economic Area'.[27] Lorber appears to concur, advising that the narrow interpretation of 'personal data' is "quite possibly rendering the UK in breach of its obligations to transpose the Directive to domestic law".[28] Indeed, following the *Durant* case, the EC issued the UK with a formal warning with regard to the DPA and its failure to conform to the Directive. In particular, the EC were believed to take issue with the definition of 'personal data' as interpreted in the *Durant* judgement.[29]

Rempell meanwhile has comprehensively discredited the Court of Appeal's judgement in *Durant*, claiming that the judgement sought to stop one specific type of subject access request but in doing so has had a far wider impact upon data protection and privacy than anticipated. He explains that "*Durant's* deviation from the Directive framework is unquestionable... the fault for these deviations lie with the court, not the underlying statute".[30] Moreover, Rempell (2006) argues that "Durant directly contradicts many guiding points made by the Information Commissioner'[31] before concluding that 'the intersection between personal data and access rights needs greater understanding and warrants further consideration".[32]

With regards to *Durant's* findings concerning a 'relevant filing system', Jagessar and Sedgwick (2005) have expressed some concern that according to the court's interpretation, "organisations that hold information in manual files which do not resemble a computerised system may... find that, following Durant, the scope of information that they are required to disclose in response to an access request has been narrowed".[33] Similarly, Lorber (2004)

[25] European Union (2007) 'Article 29 Data Protection Working Party – WP136: Opinion 4/2007 on the concept of personal data' available online at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[26] Chalton, S. (2004) 'The Court of Appeal's interpretation of "personal data" in Durant v FSA – a welcome clarification, or a cat amongst the data protection pigeons?', *Computer Law and Security Report*, 20(3): 175-181, at p. 175.

[27] Chalton, S. loc. cit. (2004) p. 176.

[28] Lorber, S. (2004) 'Data Protection and Subject Access Requests', *Industrial Law Journal*, 33(2): 179-190, at p. 189.

[29] Jagessar, U. and Sedgwick, V. op. cit. (2005).

[30] Rempell, S. (2006) 'Privacy, personal data and subject access rights in the European Data Directive and implementing UK statute: Durant v Financial Service Authority as a paradigm of data protection nuances and emerging dilemmas', *Florida Journal of International Law*, 18: 807-842, at p. 840

[31] Rempell, S. op. cit. (2006) p. 840.

[32] Rempell, S. op. cit. (2006) p. 841.

[33] Jagessar, U. and Sedgwick, V. op. cit. (2005) p. 507.

describes the notion that manual data files should resemble a computerised system as "an unachievable ambition"[34] and questions the clarity of this section of the *Durant* judgement.

Surveillance and access rights: codes of practice at national level (CCTV and credit rating)

Despite the widespread use of CCTV in the UK, the legislative instrument which addresses CCTV remains the DPA 1998 and there is, to date, no specific legislation which exclusively concerns the use of CCTV and the impact upon data protection and privacy matters. Several commentators have questioned the impact of the *Durant* judgement specifically upon the use of CCTV and subject access rights in this context. Before *Durant*, the assumed wide interpretation given to 'personal data' appeared to affect all CCTV operators and ensured that these data controllers fell under the requirements of the DPA. Post-*Durant* however, Edwards (2004) argues that 'the scope of what falls within DP regulation in terms of CCTV suddenly looks very different'.[35] Responding to these concerns, the ICO released guidance notes taking into account the *Durant* findings and whether CCTV coverage would be subject to the DPA given the Court of Appeal's guidelines relating to 'biographical' data and the 'focus' of such data. By way of example, the ICO advised that data controllers would be unlikely to be subject to the DPA if they:

- "Only have a couple of cameras
- Can't move them directly
- Just record on video tape whatever the camera picks up
- Only give the recorded images to the police to investigate an incident in their shop"[36]

The DPA appears therefore to affect more sophisticated CCTV schemes which have the ability to zoom in and out, follow individuals' movements and which are aimed at learning about a particular person's activities.[37] Edwards sums up that "what will really matter, in practical terms, is the intentions and goals of the CCTV operator when he or she sets up the cameras, and how this is translated into the physical set up and management routine of the system".[38] In June 2013, the Home Office released a 'Surveillance Camera Code of Practice' as guidance for data controllers in their use of CCTV. The code was developed in partnership with the ICO and outlines that "the purpose of the code will be to ensure that individuals and wider communities have confidence that surveillance cameras are deployed to protect and support them, rather than spy on them".[39] The code goes on to state twelve guiding principles which are intended to act as 'golden rules' for data controllers to propagate a sense of 'surveillance by consent'[40] with subject access requests briefly mentioned as part of the

[34] Lorber, S. op. cit. (2004) p. 184.
[35] Edwards, L. op. cit. (2004) p. 345.
[36] Information Commissioner's Office, quoted in Edwards, op. cit. (2004) p. 346.
[37] Information Commissioner's Office (2008) 'CCTV Code of Practice' available online at https://www.ico.gov.uk/Global/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx
[38] Edwards, L. op. cit. (2004) p. 347.
[39] Home Office (2013) 'Surveillance Camera Code of Practice' p. 5, available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf
[40] Home Office, op. cit. (2013) p. 5.

accessibility of data discussion within 'Principle 7'.[41] The concept of surveillance by consent is elaborated upon in the Home Office guidelines, which explain that:

> "Surveillance by consent is dependent upon transparency and accountability on the part of a system operator. The provision of information is the first step in transparency, and is also a key mechanism of accountability. In the development or review of any surveillance camera system, proportionate consultation and engagement with the public and partners (including the police) will be an important part of assessing whether there is a legitimate aim and a pressing need, and whether the system itself is a proportionate response. Such consultation and engagement also provides an opportunity to identify any concerns and modify the proposition to strike the most appropriate balance between public protection and individual privacy."[42]

In the UK, Section 7 of the DPA 1998 also requires that subject access requests concerning credit rating checks must be processed within 7 days and at a cost of £2 per request (as opposed to 40 days and £10 for the majority of other requests). This evidently reflects a desire in the drafting of the legislation to facilitate access to financial assessments undertaken concerning individuals.

The promotion of access rights by DPAs and national authorities and their role in ensuring compliance to national norms

In the UK, the DPA specifically charges the ICO with a duty to promote good practice under Section 51 of the Act. As such, the ICO provides extensive guidance to citizens in how to exercise subject access rights. The information is found on the ICO's website and presents a step-by-step guide outlining how to make a request, what type of response to expect (and within what timeframe) and what to do if the response is unsatisfactory. The same page also provides downloadable letter templates for citizens to use in requesting information in order to ensure that requests are made in the clearest and most detailed format.[43] Other pages on the ICO's websites outline the definitions of personal data (as per the definitions of the 1998 Act) as well as exemptions and information regarding responsibilities of data controllers in dealing with personal data and responding to subject access requests.

The ICO also maintains a register of data controllers which is available to the public via the ICO's website. The DPA 1998 demands that every organisation which processes personal data must register with the ICO (unless they fall within an exemption category) and failure to do so is a criminal offence[44]. The ICO's website explains that over 370,000 data controllers appear on the register and the information contained includes the name and address of the data controller together with a short description of the type of processing undertaken[45]. Whilst this is a good system in theory, in practice the register may be said to fail to encompass the vast variety of different types of data collection by different organisations. So

[41] Home Office, op. cit. (2013) p. 17.
[42] Home Office, op cit. (2013) p. 4.
[43] Information Commissioner's Office (2013a) 'Find out how to access your personal information' available online at http://www.ico.gov.uk/for_the_public/personal_information.aspx
[44] Information Commissioner's Office (2013b) ''Register of data controllers' http://www.ico.org.uk/what_we_cover/register_of_data_controllers Accessed 6 August 2013
[45] Information Commissioner's Office, op. cit. (2013b).

whilst the register of data controllers is certainly a positive facet of the ICO's work, it is not fool proof and citizens cannot always locate the correct contact details of a data controller.

The ICO website also provides an online complaint resolution service whereby citizens may outline the nature of their complaint and submit these via email directly to the ICO who will then begin the complaints procedure and undertake a case investigation. According to the ICO's 2012/13 Annual Report[46], in this period the ICO received 13,802 complaints, an increase of 6.3% on the previous year's total[47]. The most frequent reason for complaints relates to subject access issues – this represents 47% of complaints received. Disclosure of data is the second most frequent reason for complaints (19% of complaints) and inaccuracy of data third (16% of complaints)[48]. Of their active casework, over 80% of cases handled by the ICO are less than 90 days old. This suggests that cases are handled reasonably promptly and long, drawn out cases are rare[49].

Role of national DPAs in ensuring that data controllers allow citizens to exercise their access rights

As outlined above, the Home Office together with the ICO have provided some guidance to data controllers with regard specifically to guiding principles in use of CCTV. The ICO has provided considerably more detailed guidance in the form of a consultation paper entitled 'Draft subject code of practice', which aims to provide clear assistance to data controllers in how to fulfil their responsibilities.[50] The document extensively stipulates the legal duties imposed upon controllers and helpfully breaks down the subject access request process from general definitions, recognising subject access requests, retrieving data and responding to requests bearing in mind potential exemptions. The draft code of practice also suggests best practice examples and encourages data controllers to take a pro-active and transparent approach to responding to subject access requests. However, the document concedes that its status is limited as it outlines that:

> "Compliance with our recommendations is not mandatory where they go beyond the strict requirements of the DPA. The code itself does not have the force of law, as it is the DPA that places legally enforceable obligations on organisations".[51]

As such, the best practice advice provided by the code which evidently goes beyond the 'bare legal requirements'[52] of the 1998 Act are optional and data controllers retain the ability to follow their own procedures.

The ICO also undertakes a range of other activities in order to ensure that data controllers remain compliant with data protection law and allow citizens access to their personal data. The ICO's website includes an easy to follow online registration system for data controllers

[46] Information Commissioner's Office (2013c) 'Information Commissioner's Annual Report and Financial Statements 2012/13' http://ico.org.uk/about_us/performance/~/media/documents/library/Corporate/Research_and_reports/ico-annual-report-201213.ashx
[47] Information Commissioner's Office, op. cit. (2013c) p. 19.
[48] Information Commissioner's Office, op. cit. (2013c) p. 21.
[49] Information Commissioner's Office, op. cit. (2013c) p. 20.
[50] Information Commissioner's Office, op. cit. (2012).
[51] Information Commissioner's Office, op. cit. (2012) p. 5.
[52] Information Commissioner's Office, op. cit. (2012) p. 5.

to apply to be included in the register of data controllers (described above). This section of the website includes a step-by-step process for organisations to determine whether they fall within the remit of the DPA 1998 and therefore whether they need to become part of the register. The ICO also carries out audits, advisory visits and assessments of organisations in order to ensure their compliance with data protection principles. Summaries of these activities are available on the ICO's website, enabling transparency and accountability with respect to the advice given to organisations during the ICO's supervisory activities.

Finally, the ICO may also take enforcement action against organisations which they deem to be in breach of the DPA 1998. In 2012/13, monetary penalties were handed out to 23 different organisations, representing a total of £2.6 million[53]. In July 2013, the ICO issued the Hertfordshire Constabulary with an Enforcement Notice ordering them to take remedial action against the 'ring of steel'[54] that the police force had erected around the town of Royston in the form of a number of ANPR cameras. Following several complaints from the public, the ICO investigated the matter and found that 7 static ANPR cameras located at 6 entry roads into the town effectively meant that it was 'impossible to drive into or out of Royston without passing an ANPR camera'.[55] As a result, the ICO found that the Hertfordshire Constabulary were both processing personal data unlawfully as well as processing excessive amounts of personal data. The ICO ordered the police force to either stop the processing of the data or provide the ICO with a justification for the existing practice. This justification would need to be in line with the data protection principles of the DPA 1998. The case remains ongoing pending the response of the Hertfordshire Constabulary. Although this case does not concern subject access specifically, it is nevertheless an example of the ICO's pro-active approach to ensuring data controllers comply with the data protection legislation in England and Wales.

With regards to the ICO's enforcement activities in 2013/14, the organisation's website provides latest figures which show that, with the final year's quarter still in progress, 1,427 enforcement cases where completed in this period[56]. Of these, 1,252 cases resulted in remedial action being identified following an investigation by the ICO. 15 monetary penalty notices were applied while eight enforcement notices were served. Seven organisations were also prosecuted as part of the ICO's enforcement actions[57].

[53] Information Commissioner's Office, op. cit. (2013c) p. 32.
[54] Espiner, T. (2013) 'Police number plate camera scheme broke law in Royston', *BBC News*, http://www.bbc.co.uk/news/technology-23433138
[55] Information Commissioner's Office (2013d) 'Data Protection Act 1998 – Supervisory Powers of the Information Commissioner – Enforcement Notice – Dated 15 July 2013' http://www.ico.org.uk/~/media/documents/library/Data_Protection/Notices/hertfordshire-constabulary-enforcement-notice.pdf p. 1.
[56] Information Commissioner's Office (2014) 'Enforcement performance' http://ico.org.uk/about_us/performance/enforcement_performance
[57] Information Commissioner's Office, loc. cit. (2014)

LOCATING THE DATA CONTROLLER IN THE UNITED KINGDOM

Introduction

This country profile summary concerns the experiences encountered whilst attempting to locate data controller contact details whilst researching 34 UK-based sites. The examples below are illustrative of the individual researcher's experiences and do not claim to reflect the practices of *all* data controllers in the UK. Nevertheless, some general trends are noted alongside examples of good and bad practices encountered during the course of this research.

Methodological thoughts[58]

The sampling for this phase of research is made up of the type of personal data which may be captured about a lay person as they go about their everyday life. As such, nine domains were established which were: health; transport/holidays; work; education; finances; leisure; communications; consumerism; civic engagement. Within these domains, specific research sites were identified depending on the individual country. For example, within the domain of health in the UK, the specific sites of the nationally-held and locally-held health records were identified. The sampling strategy envisaged was divided in three ways: firstly, researchers would pick the site located geographically closest to their place of work (i.e.: the school located closest to their place of work). If this did not apply, researchers would secondly pick the site they would usually use (i.e.: the search engine they would usually use). Finally, if this did not apply, researchers would thirdly pick the national market leader (i.e.: the insurance provider national market leader).

Data controller details were most often located online through individual organisations' official websites. In the case of CCTV systems, the prominence of CCTV signage meant that in all but one site (CCTV in a local shop), we were not required to speak to any members of staff in person as signs contained a contact telephone number (supposedly) for the data controller. However, when we spoke to members of staff on the telephone, a general lack of expertise about data protection and access rights was evident. These conversations proved difficult due to the systematic suspicion of respondents who appeared sceptical that we wished to access our personal data simply because we were curious. On the two occasions that we were able to speak to data protection experts (Data Protection Manager at the local authority and Compliance Manager for the political party), their level of knowledge was excellent and we were not questioned as to our intentions. Finally, the use of emails was often necessary in tracking down data controller contact details. In several cases, telephone calls either went unanswered or no telephone number was provided which naturally led to the use of emails or, in other cases, the submission of an online query form.

Some of the research sites had to be visited more than once as attempts to locate the data controller failed in several cases at the first instance. The reason for these failures often appeared to be linked to the suspicion of members of staff who were unsatisfied that our

[58] Following the completion of this phase of the research, the UK government continued to develop a new service which sought to amalgamate a large number of public sector website into a central online platform known as GOV.UK. The government has argued that the introduction of this service will not only be significantly cheaper to administrate (allegedly a saving of £70 million per year) but will also provide a more efficient service to the public. The sites affected as part of this research were the vehicle licensing agency and the passport and immigration agency. Following the conclusion of this research, the websites of these two agencies were transferred to the GOV.UK platform. As a result, an annex has been added to this report which details our attempts to locate data controller information under the new website designs of these agencies.

'curiosity' was sufficient to allow access to our personal data. As a result, a 'second round' of visits to failed sites was undertaken during which we asserted that we wished to exercise our 'legal right' to know who the data controller was for a given site. It was envisaged that this would alert members of staff that they should seek advice from supervisors and carefully check their privacy policies before responding to our request. Where applicable, the distinction between responses from first and second rounds of visits is outlined below.

Overall impressions

Data controller contact details successfully identified in first round of visits	27 of 34 cases (79.5%)
Data controller contact details unable to identify in first round of visits	7 of 34 cases (20.5%)
Total number of data controller contact details successfully identified after second round of visits	28 of 34 cases (82.5%)
Total number of data controller contact details unable to identify after second round of visits	6 of 34 cases (17.5%)
Contact details identified via online privacy policy	17 of 28 (successful) cases
Contact details identified after speaking to member of staff on phone/via email	10 of 28 (successful) cases
Contact details identified after speaking to member of staff in person	1 of 28 (successful) cases
Average rating given to visibility of privacy content online	2 – Adequate
Average rating given to the quality of information given by online content	2 – Adequate
Average rating given to visibility and content of CCTV signage	2 – Adequate
Average rating given to quality of information given by staff on the telephone	1 – Poor
Average rating given to quality of information given by staff in person	2 – Adequate

In the first round of visits, data controllers were identified in 27 of 34 cases. Of the 27 successful cases many of these were identified with relative ease. This included research sites concerning potentially sensitive data such as national and local data controllers holding health data and schools holding data on children. Of the seven cases in which data controller details could not be found, there were six instances in which a query was made to the organisation but no response had been received after at least four weeks (this is considered as a non-response). As explained above, failed sites from the first round of visits were re-visited and our 'legal right' of access was explicitly mentioned as the reason for our request. After second round visits, we were successful in just one of the previously seven failed sites (CCTV in a transport setting). Two sites still explicitly refused to provide data controller contact details (loyalty card scheme for a department store and CCTV in a bank) while one continued to not respond at all (environmental NGO). Finally, two of the organisations responded but appeared to (deliberately?) misinterpret our query and provided us with insufficient information (Facebook and Microsoft). Overall therefore, after both first and

second round visits, we were successful in 28 of 34 sites researched. In other words, in just under one-fifth of cases, we were unable to locate a data controller.

Online content

Of the 28 successful cases, data controller contact details were located by accessing online content such as organisations' privacy policies/statements in 17 instances. In only one research site did an organisation operate its own website without a privacy policy (environmental NGO). All other research sites included privacy policies which provided varying degrees of detail on how, why and what type of information is collected and how applicants may access their personal data. The visibility of online privacy policies was generally rated as adequate – whilst most policies were located at the bottom of web pages in very small font, it is also fair to say that this is usually where the lay person may look when searching for the legal 'small print' online. In other words, whilst privacy links weren't given much prominence on web pages, they were located where one might expect to find them. The quality of the information contained within online privacy policies various widely from poor to good. Public sector websites rated higher in the quality of the privacy information provided with the majority of cases achieving a rating of 'good'. The vast majority of private sector organisations achieved ratings of 'poor' and 'adequate' with only two cases rated as 'good' ((mobile phone carrier) and the charity organisation).

It is difficult to make general comments on public and private organisations as individual approaches differed from organisation to organisation both state-sponsored and non-state-sponsored. For example, several government agencies provided templates for users to make subject access requests whilst others did not. Similarly, some private consumer organisations provided templates while others did not. The only uniform feature of all research sites (with a singular exception)[59] was that all websites included some form of privacy policy/statement.

Regarding negative practices, a number of online privacy policies displayed the following approaches to privacy matters and specifically access rights:

- Internet service provider, online gaming company, bank, insurance provider – Access rights not fully explained and key information omitted such as:
    - required format of request
    - specific reference to £10 statutory cost
    - statutory timelines
- Credit rating company – Access rights mentioned but lacking details as to how to make a subject access request and failure to give data controller contact details.
- Trade union – Failure to mention access rights at all.
- Microsoft (email provider and search engine) – Mis-interpret (deliberately?) access rights and substitute this for the right to amend incorrect information held by the organisation.

These strategies are discussed below under the heading of 'strategies of denial'. The research found that such discourses are used in various ways across different types of organisations but are most prominent in the private sector. These approaches appeared at times to be a deliberate attempt to meet the minimum legal standard of informing users of their access rights whilst still restricting the exercise of this right by failing to divulge necessary

[59] The environmental NGO did not include a privacy policy/statement on its website.

information (such as how to make a subject access request or where to send such a request to).

Public

Strategies of facilitation

In terms of government/public agencies within the sites researched, local/regional organisations tended to show best practice. For example, the local authority's online content boasts several pages regarding the collection and use of personal data as well as detailed guidance on how to make a subject access request. Moreover, a subject access request template is provided as well as a comprehensive FAQ section which includes information on the costs of making a request, timelines for the data controller to reply and the appeals/complaints procedure if required. This level of detail was exceptional and indeed was unrivalled in the rest of the research sites.

The Police similarly offered comprehensive details of their privacy policy including a six page document outlining the type of data collected and listing the various rights held by individual in terms of determining how their data is collected and stored. The agency also provides two different types of subject access request templates depending on the type of data requested and gives information on the costs of making the request, the identification required to do so and the timeline for the data controller to respond.

At a national level, the agency responsible for border control demonstrated best practice in their online content. As with the above examples, the depth of information provided about the agency's privacy policy was excellent and included a separate document outlining the agency's information charter. The content relating specifically to subject access requests was clear and detailed and included, as with the examples above, instructions on the cost of making a request, the type of identification required and the 40 day response time of the data controller. A particularly helpful template was also provided which included several 'tick box' sections to ensure that requests are made very clearly which, in theory, should help to minimise delays in the successful completion of such requests.

Strategies of Denial

The public sector did not generally appear to use methods which could be termed as strategies of denial. However, in one instance inaccurate advice was given by a member of staff evidently unaware of data protection legislation despite working in a CCTV control room. This occurred as part of attempting to locate the data controller for CCTV in a public space. We located the local authority's CCTV signage and rang the contact telephone number given. This initially took us to the 'Parking Department' who, having listened to our request, transferred us to the CCTV control room. The member of staff here simply advised, after some deliberation, that we 'write a letter and we'll see what we can do'. Unsatisfied by this response, we located the Data Protection Manager's contact details on the local authority's website and were able to speak to this officer at length about our request. Her level of knowledge was excellent and she rectified the incorrect information we had earlier been given by identifying herself as the data controller for all CCTV footage captured by the local authority.

Private

Strategies of facilitation

In the context of private organisations, examples of *best* practice in the public sector were not matched although some organisations nevertheless showed *good* practices. For example, the mobile phone carrier's online content was reasonably comprehensive and explained what type of information is collected and why. The same webpage also had a clearly defined section entitled 'Your Privacy Rights' which included a section regarding subject access requests. Within this section a template was provided which, although fairly basic, provided applicants with a standardised and simple method of making a request for personal data.

Elsewhere, the charity organisation demonstrated reasonably good practice. Their online privacy content includes an adequate level of detail on how, why and what type of personal data is collected. More specifically, the webpage also offers a direct postal address to the 'Data Protection Manager' and mentions the 40 day timeline for a response. Finally and perhaps most significantly in terms of good practice, the organisation does not charge applicants for subject access requests. Of the research sites visited, this (together with Interpol) was the only instance in which no fee was charged.

Strategies of Denial

With regards to interactions with members of staff in person or on the phone in the private sector, several instances occurred in which incorrect or inaccurate advice was given by respondents lacking expertise in data protection and access rights. This is discussed in greater detail in the context of CCTV below.

Moreover, a repetitive feature of our interactions with members of staff was what appeared to be systematic suspicion with regards to responding to data protection and access rights queries. In all cases in which we spoke to a member of staff without any recognisable data protection expertise, we were questioned as to *why* we wanted access to our personal data. As per the methodological underpinning of this task, we did not reveal our research background and maintained that we were merely curious as to whether we were allowed to access our personal data. This response bred suspicion and scepticism from respondents and on two occasions we were told that such a reason was not sufficient to allow us access to our personal data (these examples are further discussed below in the context of CCTV). We were repeatedly told that personal data is usually only released in instances where a crime has been committed and the police have requested the personal data themselves. This repeated suspicion/scepticism became especially problematic during a telephone conversation with the operator of CCTV in a transport setting, during which the respondent, despite having a generally good level of knowledge about subject access requests (i.e.: cost, timelines), was extremely reluctant to divulge the data controller's contact details and eventually demanded our home addresses and advised that he would 'send the requisite form in the post and it should arrive in due course'. This was not received after four weeks and consequently classed as a non-response. As a result, a second round visit was undertaken whereby we emailed customer services and mentioned our legal right of access. We received a response the same day which included an apology for the lack of response. Three days after receiving this email, we received a lengthy cover letter and a blank subject access request form to complete with detailed guidance and a direct postal and email address as well as a telephone number for the company's Data Protection Officer. The general reluctance to allow access to personal data without 'valid' reason suggests two things: 1) the organisations researched do not have experience of receiving many subject access requests/queries which suggests that this is an

under-utilised right and hence 2) there is a general lack of expertise in terms of how to respond to such queries correctly and according to the legal guidelines (i.e.: legislation states that applicants do not need to give a reason for requesting their personal data).

In terms of specific research sites, banks did not exercise particularly good practice. The example of one of these banks and their CCTV advice is further discussed below. Elsewhere, attempting to locate the data controller via another bank's website proved difficult. The 'Privacy and Cookies' link located on the homepage provides very limited privacy information and completely omits any reference to access rights. Having logged into our personal accounts, a new link was available at the bottom of the webpage entitled 'Legal' – a generic and considerably broad term. The link creates a pop-out window (a potential problem for users with pop-up blockers) and the information contained is limited insofar as there is little detailed explanation of data protection principles beyond nonspecific statements such as 'Your information comprises all the details we hold about you and your transactions, and includes information obtained from third parties'. Discussion of access rights is relegated to a single sentence which advises that applicant may apply for their data and gives two addresses depending on the type of data requested. Finally, applicants are advised that a fee may be payable without being told exactly how much. Timelines for response are completely omitted. Taken together, all these factors point to what may be regarded as bad practice in terms of the online content provided by the bank.

The online privacy content of multnational organisations was also a repeated source of frustration because these policies were circular, brought the user back to the same content time and again. Ultimately, we failed to identify the company's data controller/data protection department from any of these links. The privacy policies of large corporations such as Facebook and Google have been extensively discussed elsewhere[60] and this brief overview will not attempt to repeat the depth of these studies. There are however, several pertinent comments to note, particularly concerning how access rights are dealt with by these organisations. In the case of Microsoft, (which was encountered whilst considering Bing and Outlook) the privacy policy contains several online pages of information regarding how and why personal data is collected. However, considering specifically the content on access rights, Microsoft's privacy policy appears to (perhaps deliberately?) misinterpret this to mean the right to correct inaccuracies rather than the broader right to access personal data which is being processed and stored. As a result, Microsoft instructs users in how to correct inaccurate personal information but does not specifically identify nor provide any contact details for its data controller and/or data protection department. Having failed to locate a postal or email address for Microsoft's data controller despite searching through several pages of content including FAQs, we attempted to locate some way of contacting Microsoft to ask them directly. With no telephone number available, we used a virtual conversational platform located within the 'Contact Us' section of the website. Having asked the virtual respondent for a postal or email address for the data controller, we were given an address in the United States. We asked for final clarification that this was indeed the address to which we could make a subject access request whereupon the respondent apologised for what he called 'a

[60] Amberhawk (2012) An Analysis of Google's Privacy Policy and Related FAQs http://www.amberhawk.com/uploads/Google_privacy_docs.pdf (Accessed 19 May 2013); PRESCIENT (2012) Deliverable 3 – Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data http://www.amberhawk.com/uploads/Google_privacy_docs.pdf Accessed 19 May 2013

typo' and after several minutes, we were given a link to Microsoft's privacy web form with which one can submit a privacy-related query. We completed and submitted this form and received a message that Microsoft would attempt to reply within 24 hours. Within 24 hours, we received an emailed reply which had copied and pasted sections from Microsoft's online privacy policy and completely failed to answer our query. We replied stating that our query had not been answered but no reply from Microsoft had been received after four weeks and was therefore classed as a non-response.

As a result, a second round visit was undertaken. We sent another email to Microsoft at the address which had previously replied to our privacy query and we repeated our request, mentioning our legal right and outlining that we were unsatisfied with their previous reply. We received a reply within 24 hours which again included lengthy copies of the text available from the company's online privacy policy. This included information on the various instances when Microsoft may send users emails such as when they are conducting surveys or to advise customers of specific technical issues with the products they use. The content also included instructions on how users may amend their communication preferences in order to stop receiving marketing and similar emails. In other words, our request was again completely ignored.

Attempting to locate contact details for Facebook's data controller was a similar experience. Facebook's privacy policy can be located through their 'Data Use Policy'. This is reasonably extensive and covers the expected subjects of how data is collected, used and stored as well as explanations of cookies and targeted advertising. Frustratingly however, Facebook deals with the topic of access rights by providing users with an online tool to download their personal data themselves. As extensively outlined by the website www.europe-v-facebook.org, this download tool is insufficient and reportedly provides users with only 29% of their actual data (Europe v Facebook, 2013). Whilst Facebook provides both US and European postal addresses for *general* privacy queries, it fails to identify these addresses as being *specifically* those of the data controller and/or the data protection department. Two online query platforms are however, available by following links in the 'Data Use Policy'. The first of these platforms is a general privacy query web form and having submitted our query, we received an instantaneous automatic emailed reply with several links to Facebook's 'Data Use Policy' available online. In other words, the content of our query was completely ignored. We replied asking for the contact details of Facebook's data controller and no response had been received after 4 weeks and this was consequently classed as a non-response.

The second of these web forms is accessible by clicking another two links away from the Data Use Policy. Crucially however, the form itself only appears on screen once users tick a box indicating that they have an active Facebook account but cannot access it. The form then requests users' contact details as well as requiring users to upload photo ID. The form also provides an email address for data requests. This form *appears* to be a valid platform through which to submit subject access requests. However, this web form is located very obscurely and, as outlined above, only appears once users confirm that they *cannot* access their personal account (which is unlikely to be the case in the majority of instances). The obscurity, ambiguity and ultimately the failure to clearly identify the data controller and/or data protection department and its contact details appear to demonstrate not only bad practice on Facebook's behalf but also bad faith.

Given our failure in locating Facebook's data controller in the first instance, we undertook a second round visit to this site by sending both a letter to the company's Irish postal address as well as an email to the 'data request' address above. In doing so, we asked Facebook to provide us with the contact details for its data controller, mentioned our legal right of access and outlined that we did not wish to use their online self-retrieval download service. Two days later we received a reply from Facebook. The emailed reply outlined the ways in which we can retrieve our personal data ourselves by following the download tools provided in our personal Facebook account. This information is available in Facebook's 'Data Use Policy' and we had specifically stated in our query that we did not wish to use this method but were seeking the contact details specifically for the company's data controller. In other words, our query was ignored and we were provided with the content already available online. Interestingly, we received a further email from Facebook four days later in which our query was specifically answered. The email explained that the *only* way for users to obtain their personal data was via the self-download tool provided by Facebook. Furthermore, it was claimed that 'this process is in accordance with the provisions of EU Directive 95/46/EC, and is also approved by our European data protection regulator, the Irish Data Protection Commission'. So whilst our query was finally specifically answered, Facebook continued to withhold the direct contact details of their data controller.

Broadly speaking, the online privacy content and specifically the (mis)interpretation of access rights by such important organisations as Microsoft and Facebook was frustrating in the extreme. Email queries were unanswered (in the first instance), telephone numbers were not made available and privacy policy links were repeatedly circular, bringing the user back to the same content time and time again. Given the breadth of personal data collected by these organisations, the inability to easily locate contact details for the data controller/data protection department or an online request submission platform was both exasperating and disconcerting.

CCTV and signage

The importance of CCTV signage should not be understated. As well as being good practice for CCTV operators to inform citizens that they are being filmed from a moral/transparency standpoint, the issues of legality and consent also exist. As outlined by McCahill and Norris, 'in the case of CCTV systems operating in publicly accessible space the issue of consent has been substituted by 'implied consent'. But for the system to be fair and lawful people must still be made aware that they are being monitored by CCTV and this should be through appropriate signage'[61]. CCTV signage was present in all sites visited[62]. In most cases, the signage rated well in terms of visibility insofar as the signage was prominent and, in larger sites, there was more than one sign. Indeed in the case of Ikea, for example, the CCTV signage was located on the revolving door in the main entrance and was set at eye level – in other words, the sign could not be missed. In all cases, it took less than five minutes to locate the CCTV signage. In only one case did the CCTV signage fail to give some sort of contact details for further information (the small store) (see Picture 1 below) and as a result we had to speak to a member of staff directly.

[61] McCahill, M., and C. Norris (2002) 'CCTV in Britain' *Urban Eye Project, Working Paper No. 3.* http://www.urbaneye.net/results/ue_wp3.pdf Accessed 12 June 2013, page 53

[62] The CCTV sites were the following: a transport setting; a public space such as a city centre; a large department store; a small/local store; a bank.

Picture 1: CCTV in a small store

If one accepts that signage should be reasonably expected to contain full postal contact details for data controllers, the CCTV signage rated only adequate to poor with regards to content given that only telephone numbers were provided. However, most signage fulfilled three basic requirements: a) alerting the public as to the presence of CCTV cameras; b) explaining the purpose of these surveillance measures (i.e.: for the purposes of crime prevention and safety) and; c) giving a contact telephone number for any enquiries. As demonstrated by the photos below, much of the signage was in the design of a set template which required data controllers to input their own contact details as well as the intended purpose of the CCTV. This appeared to be good practice insofar as it encouraged data controllers to input the information by providing clear spaces in which to do so. In the UK, the inclusion of such information on CCTV signage is considered to be good practice by the Information Commissioner's Office's guidelines on the use of CCTV (i.e.: informing the public of who is operating the CCTV, explaining the purposes of this and giving contact details)[63] (ICO, 2008).

[63] Information Commissioner's Office (2008) CCTV Code of Practice http://www.ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx Accessed 19 May 2013

Pictures 2 & 3: Signages from CCTV in a public space and CCTV in a large department store (details of data controller blanked out)

A repetitive problem occurred however when telephoning these phone numbers. Of the five CCTV sites researched, none of the phone numbers lead directly to a data protection officer/department or indeed to a security officer/department. All phone numbers were answered by a generic call centre or customer advisor service and this naturally led to some difficulties in obtaining contact details for the data controller. The lack of data protection and access rights expertise of the respondents was an obstacle in achieving the aims of this phase of the research. This, it is argued, can also be termed a discourse of denial by failing to provide expert (or at the very least adequate/legally accurate) advice to members of the public. For example, in contacting the telephone number given by the signage in a bank, we were told by the respondent that 'due to data protection regulation, the bank is not permitted to release any CCTV footage as this may compromise the privacy of our other customers captured in the footage'. We were further advised that CCTV footage could only be released if such a request a) pertained to a crime and b) the request was made by the police. When we gave the reason of the request as being that we were just curious, we were told this was not a sufficient reason for the bank to release CCTV and the call was terminated. During our second round visit to this research site, we called the same number and repeated our request. After explaining to the respondent that we had a legal right to access our personal data, we were put on hold while she sought advice from her supervisor. When she returned we were advised that we should go to the branch in person and we may be allowed to view the relevant footage. If this is indeed the correct procedure, it begs the question as to why the CCTV signage directs readers *away* from the branch and towards a centralised call centre.

We visited the branch for a second time and asked a member of staff if we were able to request footage of ourselves as per our legal right to do so. The member of staff informed us that she would need to speak to her manager. We asked her to ensure that she should tell her manager that we have to legal right to view the footage if he/she asks why we have made this request. Several minutes later, she returned (the manager did not come out at all) and explained that there was 'no way we would ever allow anyone to see CCTV footage'. When asked why, she explained simply that this was 'the bank's policy'. We asked her to confirm twice that this was the correct procedure and she did so.

Pictures 4 & 5: Signages from CCTV in a bank and CCTV in a transport setting

Similarly, when telephoning Ikea, the call was answered by a customer advisor who, having listened to our request, was clearly unsure how to respond and eventually simply advised that we should write to or visit the individual store in which the CCTV footage was captured and 'see what they say'. Unsatisfied by this answer, we emailed the company asking how we might obtain CCTV footage of ourselves. We received an email five days later informing us that we was not able to request and view CCTV footage. As per the example of the bank above, we were told that the only circumstances in which this would be possible would be if a crime had been committed and the police had made the request. We undertook a second visit to this site by responding to the company's latest email and stating our legal right of access. They replied two days later confirming that the advice we had previously been given was indeed correct and that we were not allowed to access any CCTV footage captured by the company.

The evident lack of expertise of the respondents often led to us receiving incorrect or incomplete information about how to request our personal data. In contrast, on the two occasions that we spoke to expert members of staff having tracked down their contact details online, the level of knowledge regarding data protection and access rights was excellent and we were not questioned about our intentions in seeking to apply for our personal data. As a result, the policy of putting generic call centre telephone numbers on CCTV signage is considered to be bad practice and essentially defeats the object of putting contact details on the signage in the first place.

Concluding thoughts

In order for citizens to exercise their right to know what personal information public and private organisations collect about them, how that data is used and who it is shared with, it is necessary for them to be able to locate the person in the organisation responsible for managing their data, legally referred to as the data controller. If they cannot do so then it is simply not possible to exercise their rights. If organisations by omission or commission thwart citizen's attempts to locate the data controller, then a fundamental safeguard,

envisaged by law-makers, is being denied. On our first attempt we were able to locate the data controller in 27 out of 34 sites. On our second attempt with the outstanding seven sites, the failure rate was reduced by one case. This was despite personal, email and telephones contact where we explicitly outlined the legal basis of our request to access our personal data. In the end were able to locate data controllers in 28 (82.5%) of the 34 sites. Many of these organisations employed strategies of facilitation. They had a clearly articulated information policy, generally available on their websites, which set out what information they collected, how it was used, and who it was shared with. They clearly identified the data controller and explained the procedures for submitting a subject access request. It is however worrying that in just under one-fifth of cases this was not possible. Sometimes this was due to inadequate staff training and poor management rather than a deliberate strategy of denial. Of more concern are those companies, which seem to deliberately prevent citizens from locating the data controller.

This was particularly prevalent in the private sector. Several strategies were utilised to deny access to data controller contact details. For example, several organisations' online privacy content did not go into enough detail to enable applicants to actually make a subject access request. It is clearly inadequate to advise users of their ability to make a request for access to their personal data but fail to tell them how or to whom the request should be made. Elsewhere, supra-national online corporations such as Microsoft and Facebook provided many pages of content regarding privacy but failed to offer users an unambiguous and simple platform through which to make access requests. Given the sheer breadth of personal data collected by these organisations, there would appear to be a deliberate strategy to deny citizens their rights to know how their personal data is being used, processed and shared. It is simply not enough to provide this information generically since the law allows citizens to know how their particular data is being processed and with whom it is being shared. Finally, In the case of CCTV systems, where signage contained a generic call centre contact telephone number, rather than the contact details of the data controller, instead of facilitating the exercise of rights, in practice, it denied them. This was because organisations had failed to train their staff as to how to correctly inform a person wanting to exercise their rights, leading to inaccurate and incorrect advice being given: denial by omission. However, in the case of one major bank, denial of rights was a matter of policy: denial by commission. This also appeared to be the case with the two online transnational organisations in our sample, who as a matter of deliberate design, refuse to reveal the identity of the data controller. In phase two of the research we will take further measures to identify the data controllers in these sites and try to assert our rights to know how our data is being used, if necessary by making a formal appeal to the Information Commissioners Office.

Annex 1 – Government website analysis post-introduction of GOV.UK service

Vehicle licensing

The newly amalgamated website for the vehicle licensing agency does not provide any privacy or data protection links on its front page. In contrast with the ease with which subject access content was located under the agency's previous website design (5 minutes and 2 clicks to locate the desired information), under the most recent website construction, it was necessary to search for the required content for 36 minutes and complete 17 clicks.

Several links proved fruitless during this search. A link entitled 'Transparency Data' directed users to a general search engine with a number of links to publications, none of which at first

sight appeared to lead to information about how to make subject access requests. The website's link to the Department of Transport's (the department under whose remit the vehicle licensing agency falls) 'Publication Scheme' meanwhile, makes no mention whatsoever of citizens' right to request their personal data via the Data Protection Act 1998. Another link directs users to the agency's 'Personal Information Charter'. This document does make explicit mention of subject access requests but fails to indicate how to make such a request and does not give any contact details whereby one may submit a request.

Interestingly, the agency's homepage gives full contact details for Freedom of Information requests and indeed provides an online platform through which to make these requests. Quite why this type of request for information is afforded such unambiguous and visible prominence while request for personal information are apparently inaccessible is unclear.

In the end, having previously located a thoroughly helpful document published by the agency regarding how to access personal data when visiting the agency's old website, we were aware of exactly which search string to enter into the search function. This did indeed present us with the document in question but the nature of the search string was so specific ('Release of information from the agency's registers) that it is questionable whether a 'lay person' with no previous experience of knowing how and where to find this document would use such a search term. Other attempts to use the search function using more generic terms ('data protection' and 'subject access') yielded several pages of results with the uppermost among these having nothing to do with data protection and subject access. As a result, the visibility of data protection links on the agency's new website was rated as poor and indeed our experience of obtaining the information we sought was generally lengthy, circular and in most likelihood would have failed had we not previously located the information on the agency's previous website.

Passport issuing agency

Since visiting the previous website of the agency responsible for issuing passports, the agency changed its name, apparently to reflect the agency's 'changing role and official status'[64]. During our previous attempt to locate subject access information, we had spent 15 minutes and completed 15 clicks while we browsed the website before eventually finding the required information.

We found an altogether more positive experience in this instance. A privacy link is clearly visible at the top of the agency's homepage, a location which breaks the norm of many website designs in placing these types of links at the extreme bottom of their homepages. This link immediately directs the user to the agency's privacy policy, a nine page document outlining what type of data is collected, for what purpose and how this can be requested. The depth of information was sufficient to enable us to rate this as 'good' whereas the previous material we had located had only achieved a rating of 'adequate'. The privacy policy also directs users to an agency-specific template for subject access requests which is the same that we had previously located. In total, we spent 4 minutes and completed 2 clicks before we were able to locate the information we sought and the prominent nature of the privacy link can be rated as having 'good' visibility (whereas the visibility of the previous link in the agency's old website design was rated as 'poor'.

[64] HM Passport Office (2013) 'Introducing HM Passport Office', available at https://www.gov.uk/government/news/passports-introducing-her-majestys-passport-office

As such, the re-design of the agency's website as part of its amalgamation into the broader online presence of government services has greatly improved the accessibility of citizens to the agency's data protection and privacy-related content.

Conclusion

The government's alleged attempts to put 'its users' needs at the heart'[65] of its design in launching the gov.uk platform seems to have developed contrasting fortunes. Despite presumably seeking to engender uniformity in the way that citizens can access information and services concerning the government's panoply of departments and agencies, the juxtaposed experiences described above demonstrate that the gov.uk platform has a long way to go in this process.

While our ability to locate information about access to personal data was greatly facilitated under the new design of the passport issuing agency, this was mitigated by the considerably difficulties we faced with regards to locating similar information via the vehicle licensing website. Such contrasting fortunes experienced on the same fundamental online platform should be a cause for concern for the designers of the gov.uk website. Privacy links should, as a basic requirement, appear on the homepage of an agency's website and the passport issuing agency's prominent placement of this link is certainly to be commended as best practice. Moreover, information which mentions subject access rights but fails to explain how to exercise them or to whom requests should be sent are, quite frankly, a waste of time and will serve only to frustrate citizens seeking to find out how they may exercise their democratic right of informational self-determination.

[65] Maude, F (2012) 'GOV.UK – The start of a new way of delivering public services', *Cabinet Office*, available at http://digital.cabinetoffice.gov.uk/2012/10/16/gov-uk-the-start/

SUBMITTING ACCESS REQUESTS IN THE UNITED KINGDOM

Introduction

This country report reflects the experiences of submitting subject access requests to 23 organisations within both the public and private sector and across a range of domains. While the results outlined below do not claim to reflect all practices and approaches of organisations in response to subject access requests, the chosen sample is nevertheless reflective of domains with and in which citizens interact on a systematic and consistent basis. Thus, the overall trends observed as part of this research may be indicative of the experiences a citizen may encounter when submitting a subject access request in the UK.

Overall summary

As part of this research, 21 individual subject access requests were submitted[66]. Some form of response was received in 19 of these cases, ranging from full disclosure of personal data to mere acknowledgement of the request. Personal data was successfully received in 14 cases. Four cases were referred to national DPAs as official complaints due to either the complete non-response of the data controller or because we believe them to be in breach of their legal responsibilities to us as data subjecys.

Of the 21 requests we sent, six concerned CCTV footage, and these generated a range of unique problems. One of these was the issue of the violation of third parties' privacy in disclosing un-edited CCTV footage. However, these cases also tended to display more simplicity insofar as the object of our requests – obtaining access to the CCTV footage – was clear. At times, in cases involving the disclosure of 'all personal data' held on organisations' databases, several follow-up enquiries were necessary in order to clarify the extent of our requests. This was particularly true in commercial settings where data such as the consumer categories in which we had been placed (which have consequential effects on the marketing material we receive), was often omitted from organisations' first responses to our requests.

	Public/Private	**Site**
1	Public	CCTV in an open street
2	Public	CCTV in a transport setting (metro)
3	Public	CCTV in a government building
4	Private	CCTV in a bank
5	Private	CCTV in a department store
6	Private	CCTV in a stadium

[66] A further 16 were submitted as part of the CCTV side study.

	Public/Private	**Site**
7	Public	Local authority
8	Public	Police criminal records
9	Public	Vehicle licensing
10	Public	ANPR
11	Public	Interpol
12	Public	Border control
13	Private	Loyalty card (food retailer)
14	Private	Loyalty card (supermarket)
15	Private	Mobile phone carrier
16	Private	Banking records
17	Private	Advanced passenger information
18	Private	Facebook Ireland Ltd.
19	Private	Microsoft
20	Private	Google UK
21	Private	Amazon

The responses received were generally of a professional standard. Even during interactions with members of staff in which respondents gave incorrect or insufficient information, this was often given in good faith. It was evident however, that respondents had not received sufficient training in data protection issues. The level of expertise and knowledge concerning data protection ranged enormously from one organisation to the next. In some organisations, some respondents displayed extensive knowledge of their legal duties in responding to access requests. In others however, they were completely reliant on our directions due to their near

complete lack of awareness of data protection and privacy legislation. As a result, although most respondents acted in good faith, those lacking the necessary knowledge of data protection compliance issues displayed a series of unwitting strategies of denial. These included giving plainly incorrect information, such as being advised that one cannot, in any circumstances, request CCTV footage. In other cases, data controllers and their representatives gave incorrect information which resulted in unnecessary delays in the submission and processing of our access requests. Such incorrect information included giving the wrong contact details for the department/officer responsible for processing access requests, failing to outline the identification requirements and cost of making a request and failing to provide proper clarification in cases where more information was required from us in order to process our request.

However, several cases of facilitative practices were also evident in both the public and private sector. Some organisations provided full and unambiguous guidance via their online privacy policies, enabling citizens to submit access requests without any delays. In a number of cases, this included the provision of detailed templates which ensured that all necessary information would be received by the data controller in a single correspondence, saving the citizen both time and money (in postage fees). However, the positive practice of providing templates was negated in some cases where these templates were only made available to us *after* we had already sent a first request. In these cases, the question arose as to why these templates are not made openly available to citizens if they are intended to help all parties process requests efficiently. The failure to make these templates openly accessible suggests some degree of denial strategy on behalf of the data controllers concerned.

Elsewhere, having received our correspondence, a number of organisations not only acknowledged our requests but pro-actively informed us of their statutory obligation to process and reply to our request within 40 days, displaying good levels of self-accountability and regulation. Such strategies of facilitation demonstrate not just compliance with the law but a pro-active effort to go beyond compliance and enter the realms of good/best practice. Moreover, in the practical dynamics of the exercise of access rights, these facilitation strategies lift the burden of time and effort away from the citizen by simplifying the request process as much as possible.

Finally, as part of our subject access requests, alongside disclosing our personal data, we asked data controllers to answer two specific questions. Firstly, how they shared our personal data and with whom they shared this with. Secondly, data controllers were asked whether or not automatic decision making processes had been used in processing our personal data and if so, how this had affected our data specifically. Data controllers responded to these queries in vastly different ways and this will be highlighted where appropriate in the case summaries below. The range of responses included completely ignoring our queries, partially addressing them but in a legally non-compliant manner, providing a legally compliant response with the bare minimum of detail and finally comprehensively explaining how and why our data is processing automatically.

Case-by-case Analysis

<u>Public – Facilitative Practices</u>

Vehicle Licensing

This case showed both facilitative and restrictive practices. From a restrictive point of view, we struggled greatly to locate the agency's data protection and privacy content via its official website. This process is extensively documented in the report concerning our attempts to locate the data controller and it is an interesting case which highlights the impact of the British government's changes to its online interface with citizens via the establishment of the gov.uk platform.

The online information indicated that two separate requests must be sent to the agency since it operates two types of databases in which personal data is stored – driver records and vehicle records. However, the online information also explains that requests for data from each database are charged at only £5 each, making a total of £10 for both databases.

Having sent our requests, we received relatively quick responses enclosing our personal data. The letters also included lengthy but seemingly formulaic outlines of the agency's obligations and commitments to data protection and privacy principles. The data received also included a specific example in which our personal data had been shared with a third party[67]. Notably, however, we had received no response concerning automated decision making processes and were therefore required to contact the agency again regarding this part of our request. Some weeks later, we received a response to our query. The letter explained that the agency uses an electronic system whereby data can be transferred to contracted parties. This however, is not an automated decision making process insofar as no decisions are made about us and we are not placed in a category during this process. This response appears to demonstrate a willingness to engage with us openly, outlining a system which, whilst electronic and automatic, is not strictly classed as operating automated decision making processes.

Generally speaking, the agency demonstrated a number of facilitative practices. The availability of data controller and access request information on the agency's website differs dramatically before and after its move to the gov.uk platform. The latest incarnation of the agency's online presence appears to bury the relevant data protection content deep within its web design, demonstrating particularly restrictive practices[68]. However, once this considerable obstacle is overcome, the agency appears to employ generally facilitative procedures. The £5 charge per request accounts for the potential additional burden placed upon data subjects as a result of the necessity to request personal data for the DVLA's two databases. The speed with which replies were received was quick and in any case well ahead of the statutory 40 day deadline. Moreover, the information disclosed included a specific example of data sharing with third parties, representing one of the only instances in this research in which a data controller has not simply provided generalised examples of when data sharing may occur and with which categories of third parties. Although it was necessary to send two further correspondences in order to receive a response to our query regarding automated decision making processes, the reply eventually received also demonstrated facilitative and transparent behaviour.

Interpol

This case showed predominantly facilitative practice with the notable exception of the difficulty of locating information via the organisation's website concerning how to make a request. The relevant data protection/subject access content was not easy to locate and we

[67] This concerned an instance in which our personal data had been shared with the police in connection with a speeding offence.

[68] See the above report for a full description of this restrictive practice.

spent 20 minutes searching for this before finally locating the relevant information. This is considered to represent very poor practice in web design and online content accessibility.

The content itself is adequate and users are advised of how to make a request, including the identifications requirements when submitting a request. Moreover, a one-page template is made available for users via which to make a subject access request. The contact address to make requests is in France which means that significant postage costs may be incurred depending on where the request is sent from. However, counter-acting this is the fact that requests are not charged (which is not the case in the UK).

Our request was sent on 11/09/13 and we received a reply on 15/10/13. This was within the 40 day response time prescribed in the Data Protection Act 1998. The reply explained that their searches had found 'no information to disclose that is applicable' to our request.

In summary, the process was reasonably straight forward once we had located the relevant information online. The presence of a template is helpful as is the clear identification of a postal address for the relevant department to whom access requests should be sent. The response time to our request was adequate and within British legal limits and the content of the responses was simple but clear. However, the initial problems in locating the relevant data controller information and contact details online acted as something of a barrier to our ability to make a request in the first place.

Police criminal records

This case showed a number of facilitative procedures and practices. We searched for the relevant data protection information via our local police service's website. The content was easy to find and took a total of 5 minutes during which we completely only 2 clicks. The level of information contained within the data protection section was good and addressed how to make a request as well as the type of information collected and stored by the organisation. Moreover, the content explained that subject access requests may be made for two types of databases: the information held at a local level by the Police, and information held at a national level by the police on the Police National Computer (PNC)[69].

The website included two templates with which citizens can make a subject access request to reflect the two databases to which requests can be made. However, citizens need only to send their requests to one (local) address and the request for information from the PNC will be forwarded automatically. This is a helpful practice and avoids citizens having to send two separate requests to two different addresses. The templates outline what type of identification must be provided and the necessary fee which ensures that requests will not be unduly delayed due to the citizen not being made aware of the full extent of the access procedure.

Both requests were sent on 11/09/13. On 13/09/13 we received an acknowledgement email from the national Criminal Records Office advising that our request was being processed. The email also detailed that the organisation had 40 days in which to respond to our request. This is an example of good practice since the data controller demonstrated self-regulation by making us aware of the legal timeline in which they must respond. The same day, a letter was received from the local Police force also acknowledging our request and once again setting a deadline for their own response time. They also provided us with a receipt for our payment

[69] For a more in-depth discussion of the level of information contained within the police's online content, see the above report on our attempts to locate data controllers.

and returned one of our cheques, explaining that it was only necessary to pay the £10 administrative fee once despite having made two requests.

We received a letter from the local Police on 26/09/13 which enclosed our personal data. The documents included all interactions we have had with the local Police to our knowledge, including calls in which we have made complaints as well as calls in which we have acted as a witness to an incident. The letter also directly addressed the fact that our personal data has not been shared with third parties and that we have not been subject to automatic decision making processes. The letter itself was sent with a requirement that it be signed for which further demonstrated good practice insofar as protecting our personal data enclosed in the letter whilst in postal transit.

We received a letter from Central Records Office on 11/10/13 which explained that we do not appear on the PNC.

In summary, the police showed good practice in processing our subject access request(s). The information contained on the local Police's website is clear and thorough and the provision of templates offers data subjects an unambiguous guide of how to make a request. The full outline of ID and payment requirements also avoids unnecessary delays in processing requests. Both our requests were acknowledged and these acknowledgements outlined the organisation's response time obligations which demonstrated self-regulation. The personal data was received in a timely manner and within the legal timelines. The data itself was, to our belief, full and intelligible.

Local Authority

This case demonstrated mostly facilitative practices. We located the necessary information on the organisation's official website quickly and easily. The privacy content online was of a good level of detail with a lengthy FAQ page outlining how to make a request together with a template with which citizens can make access requests. The template, whilst being reasonably short and simple, provides a clear procedure for citizens to make their requests and ensures that the access request is not unduly delayed.

We sent the template form together with the relevant documentation and payment on 13/07/13. Three days later on 16/07/13 we received a phone call from the organisation who wished to know if we were seeking any type of data in particular. The template had given us the option to specify that we wished to receive information either from a certain department within the organisation or choose to receive 'all' information held about us. Given that we had ticked the 'all' option, we found this phone call unnecessary and perhaps an attempt to limit their search. However, a kinder reading of the situation may simply be that they wished to respond to our request as efficiently, accurately and quickly as possible and therefore tried to avoid any unnecessary searches if we'd had a particular type of information in mind. We subsequently received a confirmation letter advising that the request was being processed and that we should expect to receive a response within 40 days. On 22/08/13 (one day within the 40 day deadline), we successfully received our personal data. This included information on our past addresses, library records and council tax payment details. We were also advised that our data had not been shared with third parties.

In summary, the data controller showed good practice in not only processing our request but also in its dissemination of the relevant information via its website which enabled us to make the request easily in the first place. The information online was clear and comprehensive and

the provision of a template avoided delays in processing our request. The self-regulation shown by the organisation was also good practice and the disclosure of our personal data was made within the 40 day legal limit.

Public – Restrictive Practices

ANPR

We drove through a location in which several ANPR cameras are in operation on 25/02/14 and located several ANPR cameras placed at various entry points in and out of the location. Signage on the outskirts of the town advises that CCTV cameras are in operation but no signage is present next to the cameras themselves and the signage does not explain that the cameras in question are ANPR-based. We subsequently visited the local police force's official website and located the privacy policy. This was not, however, a particularly easy task and it was necessary to use the search function on the website to find the content we were seeking. The privacy policy included a template with which to make access requests and we completed and sent this to the data controller on 25/02/14. The form outlined the payment and identification requirements, thus minimising potential delays in processing our request. Together with the template, we provided a detailed list including timings of when we had passed by each camera in order to provide a clear and unambiguous description of our movements through the location.

On 03/03/14, we received confirmation from the data controller that our request had been received and that we should expect as response by 09/04/14, as per the legal timeline afforded to data controllers in such matters.

On 05/04/14, a few days within the 40 day deadline, we received a reply from the police force. The letter explained that based on the information we had submitted in our request, the data controller had been 'unable to provide a positive comparison confirming you would have been driving the vehicle in question'. As a result, our request was denied. The matter of third party data sharing was directly addressed by explaining that ANPR data is strictly controlled and only shared with third parties if doing so serves a specific policing purpose. Moreover, a list of potential third party recipients was provided. Automated decision making processes were addressed in the letter by stating that the police force does not use such processes.

In denying our request, the data controller did not appear to provide us with a legitimate legal reason. No exemption categories were met and the simply conclusion that they could not confirm that we were driving the vehicle was somewhat bizarre. We had provided them with a full list of movements (with timings) and had sent all identification requirements stipulated by their own access request template. Quite how we could take further steps to confirm our identity and that we had been driving the vehicle in unclear. As a result, our right of access was denied based on unclear and ambiguous reasoning.

From a more positive perspective, the data controller did at least have a clear procedure to receive and process access requests, including the provision of a template which enabled us to make a complete request with just a single correspondence. Moreover, we received their reply within the legal timelines and the issues of data sharing and ADM processing were clearly and directly addressed.

Border Control

This case demonstrated both facilitative and restrictive practices. In considering the restrictive practices, one should note that in the time between submitting our request to receiving a first response, the public agency responsible for border control records was re-launched/re-branded following the under-performance across a range of sectors by the previous incarnation of the agency. As a result, the behaviour described below may be partially explained by the possible structural re-organisation of the data controller in the weeks/months surrounding the submission of our request.

The agency's data protection and privacy information was easy to locate via its official website and we accessed this content within three minutes. The information contained online was of an excellent level and described in considerable depth the access request process, even providing a template, offering very clear guidance and a check-list for data subjects to ensure requests are made in full[70]. The template demanded specific details of what our request encompassed as well as outlining the identification and fee requirements. This approach is considered to represent good practice insofar as it helps to avoid undue delays in processing access requests as well as providing citizens with clear advice in how to make such requests. We completed the template and posted this to the data controller's postal address on 11 September 2013.

However, some weeks later, on 4 October 2013, we received a reply from the new incarnation of the agency stating that our request could not be processed as 'you have failed to provide sufficient details to enable us to process your request'. No further explanation was provided and rather than invite us to clarify our request by sending additional information, all our documentation including the fee was returned to us. This reply was particularly puzzling given that we had completed the agency's *own* template which was presumably designed to encourage requesters to provide all necessary information for the data controller to process requests. We replied the following day asking for clarification and noting our surprise that our request had been discontinued with no attempt to resolve the matter more pragmatically.

A second letter was received from the agency on 4 November 2013 – a further month later – explaining that we should communicate our passport numbers to them in order to obtain our travel records as well as sending the £10 administrative fee. The issues with this response were self-evident: firstly, we had sent a copy of our passport in our first correspondence. Secondly, we had also sent the requested payment in our first request. As a result, all of the information required by the data controller had in fact been sent previously and returned to us as insufficient. Thirdly, the need to re-send this information meant that we had incurred not only undue delays of almost two months in processing our request but we also had to pay additional postage costs. Moreover, as a minor aside, the reference numbers for our request differed from one letter to the next potentially indicating poor administrative procedure. Nevertheless, these documents were sent to the data controller once more on 5 November 2013.

We finally received a letter from the agency on 20 November 2013, explaining that the request was now 'live' and would be processed accordingly. The letter also outlined the 40 day deadline by which the data controller was bound to reply to our request. On 12 December 2013, approximately three months after sending our first correspondence to the agency, we received our personal data together with a cover letter. The letter directly addressed the issue

[70] See the locating the data controller UK country report above for a more in-depth discussion of the border control agency's online presence and the good practice demonstrated therein.

of third party sharing and automatic decision making, explaining that neither had taken place with reference to our data. The letter also advised that a record of our access request would only be held on file for three months, meaning that our so-called data vulnerability as a result of making an access request was low. The personal data itself contained all records of our entries and exits to the UK over the several preceding years. The data included airports of exit and entry, 'travel document numbers', PNR locator numbers, flight numbers and basic biographical data.

This case perhaps perfectly demonstrates the dichotomy between the restrictive and facilitative behaviours of data controllers before and after submitting an access request. In the process of attempting to submit a request, the behaviour and responses received from the data controller were poor and the nature and content of their replies were haphazard. While one can take into account the organisational re-structure of the organisation, our ability as citizens to exercise our rights were, in this case, denied and hampered by the poor practice employed by the agency. In light of the fact that this organisation represents one arm of the Home Office, this was considered to be particularly restrictive practice, given the amount of data systematically collected by this controller and the potentially sensitive nature of this data (immigration records; travel history; law enforcement stops at ports, etc). However, once the request was finally submitted, the response received was clearly facilitative and included directly addressing the issues of third party data sharing and the use of automated decision making – one of very few data controllers to directly address this without further probing.

<u>Private – Facilitative Practices</u>

Bank Records

This case demonstrated both facilitative and restrictive practices. From a restrictive perspective, the data protection information on the organisation's website is accessible only to those individuals with an online banking account. This is poor practice insofar as it effectively means that a large amount of data subjects (i.e.: non-customers and customers without an online account) are unable to locate data controller details. The content itself is also brief, providing two contact addresses for request but no accompanying information on how to make (or what to include in) a request besides one line explaining that a fee may be applicable. In other words, the information provided is the bare minimum standard and while it may meet a minimum legal standard, it is far from significantly facilitative for customers/citizens seeking guidance in this matter.

Using the address provided in the privacy policy, we submitted an access request. We received a response ten days later from the bank's Manager of the Subject Access Request Team seeking further information including payment and identification. We replied and later received a second response advising that our request was being processed and mentioning the 40 day timeline within which the company would be replying. It also explained that we may receive several correspondences at different times as different departments would be responding to our request rather than a single department sending just one reply.

Over the following weeks, we received a series of correspondences from different departments within the organisation. Some of these confirmed that no data was held about us while others disclosed a range of personal information. A notable omission from all correspondences however, was any mention regarding automatic decision making processes. We therefore sent a further letter asking for clarification on this matter but we received no reply.

In summary, the timeliness with which the bank responded to our request was broadly speaking at a good level. The nature of the documents received appears to cover all interactions we have had with the company although it is of course impossible to know this for sure. The nature of the communication between ourselves and the Subject Access Request Team once we had successfully sent a complete access request (with fee and ID), was at a reasonably clear. However, the process of submitting a request prior to this was not as unambiguous and simplistic. The lack of detailed information online meant that we were required to send two separate correspondences before our request was considered 'complete' and could be processed. Once again, this reflects an ongoing issue with the submission process in which problems are encountered prior to submitting a request but once a request is submitted, the process becomes significantly easier. Finally, the complete failure to address our query regarding automated decision making processes is notable, particularly since the data controller's frequency of correspondences stopped somewhat abruptly when this matter was raised. The pointed silence which followed seemed to betray a clear reluctance to disclose this type of information to data subjects. In the context of a bank, automated decision making is likely to include credit checking procedures which the data controller is unlikely to wish to divulge to data subjects and the non-response to this query perhaps reinforces this conclusion.

Loyalty card (food retailer)

This case demonstrated mainly facilitative practices with minor exceptions. The privacy policy was fairly easily to locate via the organisation's website. The information contained therein can be described as adequate and the access rights section provides a reasonably good level of detail insofar as the relevant legislation is mentioned together with an email and postal address for submission of requests. However, there is no mention of identification requirements and users are only advised that 'any subject access request may be subject to a small statutory fee to meet our costs in providing you with details of the information we hold about you'.

Having submitted a request via email, we received an emailed reply from a customer service representative the following day explaining:

> 'Unfortunately, the nature of your email message is unclear to us. If you would restate the question or give more details on what information you would like, we would be happy to respond to your inquiry.'

Given that we had submitted our query to the email address provided in the company's privacy policy, this reply seemed inadequate and indeed an indication of administrative and organisational inefficiency. Simply put, why provide users with a contact point if this contact point cannot answer fairly basic queries? From a procedural perspective, this appeared to be a restrictive practice.

We replied the same day stating that we were unsure how to clarify our request and that perhaps a data protection or legal officer may be better placed to respond. We subsequently received an email some days later from a paralegal officer at the company, acknowledging our request and asking us to send identification in order for the access procedure to begin. Notably however, payment was not requested. This meant that the failure to outline in the privacy policy that identification is required caused delay in the processing of our request. We replied the same day and received a confirmation response, advising that our request would now be processed.

Some weeks later, we received a copy of our personal data, together with an explanation that none of our personal data had been shared with third parties as per the preferences we had indicated on joining the loyalty card scheme. Automatic decision making processes however, were not addressed.

The personal data itself included a number of screen prints of internal IT systems which contained basic biographical information. It also included all communications between the company and us together with a table detailing the times and dates when we used the loyalty card. Transactional information was also included (i.e.: the balance remaining on the card after use). However, merchant identification numbers were redacted which effectively meant that we were unable to determine locational data of where the card was used.

Given that automatic decision making processes had not been addressed, we emailed the data controller once more on 15 January 2014 and sought clarification on this matter. We received an emailed reply the same day explaining that:

> '(The company) does not use automated decision taking processes on your personal data in order to make decisions about you, your status or categorise you in any way.'

Generally speaking, the company demonstrated mostly facilitative practices. Despite the lack of expertise shown by the first respondent to our request, once our request was forwarded to a suitable officer, the access process was reasonably straight forward. We received fairly clear communications and weren't asked for payment. Moreover, all correspondences were conducted via email, ensuring that the process was quick. Our personal data was received within the 40 day time limit for data controller responses and the cover letter enclosed directly addressed our third party query. Automatic decision making processes were not addressed but having contacted the company about this omission, we received a same-day response with a satisfactory answer. Quite why this was not included in the covering letter is unclear and would have saved us the need to send another correspondence. However, we ultimately received all our personal data and all our queries were addressed in a satisfactory manner.

Loyalty card (supermarket)

This case showed both facilitative and restrictive practices. The relevant data protection and privacy information was easily located via the organisation's website. The privacy policy is adequate although the section concerning specifically how loyalty card data is used comprises a single sentence:

> 'We access the information recorded through the use of your (loyalty card) to help us improve our service to you and to make our communications more relevant.'

The section concerning access to data similarly lacks depth but does include the basic information needed to make a complete request with just a single correspondence. This means that the full postal address for the data controller is provided, together with mention of the £10 fee for requests and the company's identification requirements.

Having sent a request together with a cheque for £10 and details of the loyalty card's number, we received a reply enclosing the organisation's access request template. The template itself showed reasonably facilitative practices insofar as making the access request process very clear. However, the fact that the form was only available after a first correspondence had

already been sent appears to negate any potentially good practices displayed by the form itself.

We completed and returned the form and subsequently received our personal data ten days later. The covering letter advised that 'a copy of all your personal data is enclosed'. This included an explanation that our personal data had not been shared with third parties since we have indicated in the past that we did not wish for this to take place. The issue of automatic decision making however, was ignored. The personal data itself appeared to simply be a number of screen prints of information already available to us via our online loyalty card account. Indeed, it seemed only a single sheet of paper was included in the correspondence was data which was not already available to us and this sheet of paper was a screen print from an apparently internal programme containing basic biographical information about us.

With this mind, we contacted the data controller once more via email asking for clarification on automated decision making processes as well as asking if the previous correspondence included all our personal data. Almost two months later, we received another correspondence with additional personal data. The covering letter apologised for the delay in replying and explained that further to our letter, our request had been checked again and indeed, they had 'found that there was some missing information' which included details of where and when we had spent our coupons. The letter also addressed the issue of automatic decision making processes, by stating that coupons are generated based on the purchases made using our loyalty card together with the forms we had previously completed upon joining the scheme indicating our shopping habits, effectively outlining the process of customer profiling.

In summary, this case simultaneously displayed facilitative and restrictive behaviours in processing our access request. Although the information made available online is relatively clear and sufficient, the procedural practice of sending templates to requesters after an initial correspondence has already been sent means that additional costs and time delays are incurred by the requester. The company's subsequent response to our request was incomplete and it was necessary to sent further correspondences addressing this before finally receiving a complete response almost two months later – well beyond the 40 day deadline. The necessity to press the data controller for a complete response assumes a level of data protection and privacy knowledge on behalf of the data subject which places him/her beyond the sphere of a so-called ordinary citizen with little or no knowledge about what type of personal data may be held about him/her. In other words, this case appears to be an instance in which the success of an access request is restricted to those individuals with sufficient knowledge, determination and possibly resources, to pro-actively pursue the data controller until full disclosure is achieved.

Mobile Phone Carrier

This case demonstrated predominantly facilitative practices. The organisation's privacy policy can be easily accessed via its official website and the privacy link is located at the bottom of its homepage. The content of the policy itself is reasonably good, including information on the type of data which is collected, retention periods and how the data is stored. Although the information is presented in fairly broad and general terms, the majority of the expected topics are covered. This includes a section entitled 'Access to your personal information' which provides a link to a downloadable template form for making access request. The section also mentions the £10 administrative fee and offers alternative ways to receive the template if one cannot download it. With this in mind, the online content

demonstrates good practice by not only explicitly mentioning the right of access but also making available a template via which citizens can exercise this right. This demonstrates pro-activity on behalf of the data controller and a shift of burden away from the citizen.

The form itself is very basic but covers the information required for the data controller to process a request. It also ensures that requesters enclose the necessary ID and fee for the request. This allows citizens to make full and complete requests in the first instance and avoids unnecessary delays such as the exchange of correspondence asking for clarification of the request/the required fee/the required ID.

We completed and sent the form together with the fee and ID on 13/07/13. We received a package on 08/08/13 which included a cover letter and a data disc. The cover letter outlined the type of data which is held about us and explained, in general terms, the categories of third parties with whom our data is shared. The letter also explained that personal data is shared with a third party for billing purposes and in certain specific events such as the delivery of goods when companies such will be provided with our address. The disc held fairly comprehensive personal data including all our billing history, screen shots of occasions when the company has contacted us (and vice versa) and notes made by their staff of these conversations. It also included a list of outgoing call data, including geographical data of cell site hits when the calls were made.

Given that the letter had failed to address the issue of automatic decision making and had only outlined third party sharing in general terms, we emailed them on 24/10/13 asking for further explanations on these matters. We received an emailed reply the next day explaining that no automatic decision making processes are employed as the organisation's credit checking system requires manual intervention. With regards to third party sharing, the same information we had previously been given was repeated. We replied once more to this email asking for specifics regarding third party sharing but received a reply the same day which quoted the Data Protection Act 1998 and asserted that data controller are only required to provide citizens with 'categories of third parties' with whom data is shared. Under this reading of the legislation therefore, the data controller had been compliant in providing us with a general description of the types of companies who receive our personal data.

In summary, this case demonstrated fairly good practice. The information on the website together with the provision of a template represented an unambiguous and clear pathway for us to make a request, avoiding undue delays and obstacles in doing so. The response was comprehensive and timely and enabled us to receive our personal data by sending a single correspondence. Despite repeatedly asking for specific examples of data sharing, we received only general descriptions but this, it seems, is compliant according to the wording of the legislation and therefore we can only assess that the company acted in accordance with its legal obligations. As a result, one can assert that the data controller demonstrated good practice throughout the process of our exercising our access rights.

Amazon

We located a contact address for Amazon's data controller on the organisation's online privacy policy. The address was located very quickly but the remainder of the policy offers very little information about the subject access process, demonstrating possibly restrictive practices in informing customers of their access rights.

On 05/11/13, we sent a request to an address in England which was identified online as the data processor (whereas the data controller is identified as being located in Luxembourg). We received no response to this so on 27/01/14, we send a second letter advising that we would contact the national DPA if no response was received. On 13/02/14, over three months after our first letter, we finally received a reply from Amazon. This reply came via email and asked us to send our identification. We replied via email the same day with a scanned copy of our ID.

On 25/03/14, over a month since their previous correspondence and almost five months after our first request, we finally received our personal data from Amazon. This was received via email to which were attached several password protected documents (the password was sent to us in another email). The documents included a cover letter and tables of our personal data. The cover letter explained what the data encompassed and that all data had been either provided by us or had been gathered as part of our activities as a customer of Amazon. The personal data files included all our purchase history (going back to when we opened the account 10 years ago) as well as basic contact and payment details such as current and old postal addresses and payment cards.

The cover letter also addressed our queries regarding third party data sharing and automated decision making processes. Regarding third party data sharing, the letter explained that Amazon carries out such practices based on the terms of its privacy policy (and a link to this was provided). As such, Amazon addressed this matter in only general terms, demonstrating a compliance with strict legal provisions but failing to fulfil our request for *specific* examples of such practices.

With regards to ADM processes, the letter states simply that 'we do not take decisions on our customers based on automated process means'. It is rather clear however, that Amazon customers undergo some level of profiling. Amazon's denial of the use of ADM processes therefore suggests that their profiling activities are not wholly automated and some form of human intervention is involved here. It is worth noting here that Amazon's letter explicitly states a number of times that their response to our request is in line with data protection legislation and fulfils their legal duties. In the context of ADM processes, this suggests that in claiming that no such processes are carried out by Amazon, the data controller has taken an interpretation of such practices which differentiate their profiling activities from ADM processes.

This case can therefore be considered as displaying elements of both facilitative and restrictive practices. Amazon's response ultimately disclosed our personal data and addressed our questions concerning third party data sharing and ADM processes. However, these issues were seemingly addressed using interpretations which are legally compliant but shed little light on how our personal data is used from the data subject's perspective. The question arises here as to how useful the right of access truly is when one wishes to know – in detail – how his/her data is used by large multinational corporations such as Amazon. Moreover, the disclosure of our personal data took almost five months from the date we submitted our request, representing the longest time span of any successful disclosure in this study.

<u>Private – Restrictive Practices</u>

Advanced Passenger Information

Although we received our personal data in this case, the data controller's behaviour displayed restrictive practices which caused confusion and long delays in the access request process. The airline from whom we requested our Advanced Passenger Information failed to reply to two letters until we threatened them with further action via the national DPA. Once a reply was finally received – over two months after our first correspondence – the content of their response was unclear and somewhat confusing as we were asked to pay £17/20 Euro in order for our request to be processed. The reason for this payment (and more specifically the amount) was not explained in the letter and was not immediately obvious to us given that subject access requests cost £10 in England and Wales and 6,35 Euros in Ireland (where the airline's headquarters are located) according to legal guidelines. No further reply was received thereafter and we submitted a complaint to the Irish national DPA on 20/02/14 and received confirming from them on 27/02/14 that they would begin their investigation into the matter. On 21/03/14, we finally received an email from the company disclosing our personal data and advising that data is only retained for 18 months so any older data will have been destroyed. The content of the email made no reference to the DPA complaint and added to the overall confusion in this case by apologising 'should you not be in receipt of our earlier correspondence', suggesting we had missed previous letters/emails from the company. No mention was made of third party data sharing or automated decision making processes. We subsequently received an email from the Irish DPA who confirmed that as a result of the letter sent to us from the company (which they had received a copy of), they were satisfied the matter was closed.

The process of obtaining our personal data in this case was therefore arduous, necessitating a complaint to the national DPA before receiving a coherent response from the data controller. Even this response however, remained incomplete since not all aspects of our request were addressed.

Facebook

Facebook, whose European headquarters are based in Ireland, demonstrated extensive restrictive practices in our attempts to submit an access request. The data controller's privacy policy is easily and rapidly accessible via its homepage under the title 'Data Use Policy'[71]. Facebook provides users with an online tool with which they can download their personal themselves. However, we sought to submit a subject access request directly to the data controller and as such wrote to the company's headquarters on 08/05/13 as well as submitting our request via an email address located amongst the privacy-related content online. We received an emailed response from Facebook on 06/06/13, which essentially ignored the specific content of our request and instead appeared to provide us with information which was largely cut and pasted from their online privacy policy. We replied, outlining that this was insufficient since we sought to submit an access request directly to Facebook's data controller but we subsequently received a response on 10/06/13, explaining that 'The Download Your Information tool is the only way for Facebook users to access the personal data we hold about them. This process is in accordance with the provisions of EU Directive 95/46/EC, and is also approved by our European data protection regulator, the Irish Data Protection Commission'. Hence, our request would not be processed. As a result, we submitted a formal complaint to the ICO on 30/07/13.

[71] For a fuller assessment of Facebook's privacy content, see the UK's locating the data controller report.

We received a rapid response from their complaint resolution team explaining that since the company was based in Ireland, they were subject to Irish law. With our consent however, our complaint was forwarded to the Irish DPA, the Office of the Data Protection Commissioner (ODPC). Some weeks later on 26/09/13, we received a lengthy email from the ODPC explaining that they were satisfied with Facebook's privacy practices and indeed the ODPC had worked closely with Facebook in designing their privacy tools and content to ensure that they were faithful to the national legislation. Moreover, they concluded that 'it is our position that there is no personal data that can be supplied by FB-I (Facebook Ireland) that is not now available to users and we are satisfied that this mode of providing access to personal data satisfies their obligations to provide access to personal information under Irish data protection legislation'.

We replied on 24/10/13 explaining that, alongside our personal data, we wished to know with whom our data had been shared and whether it had been subject to any automatic decision making processes. The ODPC replied once more on 30/10/13 advising that firstly, if we knew Facebook had shared our data with third parties we should explain this and the ODPC would investigate further. Secondly, they explained that Irish data protection law did not entitle us to know about Facebook's automatic decision making processes but rather we were only entitled to a copy of our personal data. Two crucial issues arise here: firstly, a citizen cannot know an unknowable, hence the reason for a subject access request. The ODPC's advice for us to inform them if Facebook has shared our data with third parties is nonsensical since the reason we were requesting this is precisely because we do not know (but have a reasonable suspicion that they have done so). Secondly, the EU Directive 95/46/EC expressly allows citizens to request from data controllers details of their automatic decision making processes and as such, the ODPC's response that Irish law does not entitle us to this raises possible matters of non-compliance of national legislation with European law. We replied to the ODPC on 20/11/13 outlining these concerns.

On 24 December 2013, we received two emails directly from Facebook. The first concerned the issues of third party data sharing and automated decision making processes. Regarding third party data sharing, the email explained that data is shared as part of users' use of applications, games and external websites. During such interactions, Facebook 'give the game, application, or website your basic info, which includes your User ID and your public information. We also give them your friends' User IDs (also called your friend list) as part of your basic information'. The email also explained that users can alter their data sharing settings within their 'apps' settings, enabling them to take 'complete control' by allowing 'you to see the permissions you have given the applications, the last time they application accessed your information, and the audience on Facebook for timeline stories and activity the application posts on your behalf. You can also remove applications you no longer want, or turn off all Platform applications'. One may question here why such a seemingly central and important privacy setting tool is located in a somewhat specific 'apps' section rather than the user's more encompassing sections such as 'General' or, more to the point, 'Privacy' sections.

Regarding automated decision making processes, the email confirmed that no such processes had taken place in relation to our account. In general terms, the email explained that information provided by users may be used to provide targeted services including using users' GPS data to provide location-specific information and services.

The second email we received referred us back to Facebook's self-download tool and encouraged us to use this service in order to obtain a copy of our personal data, helpfully reminding us that 'Your downloaded file may contain sensitive information. You should keep it secure and take precautions when storing, sending or uploading it to any other services'.

Since no further correspondence was received from either Facebook or the ODPC a month later, we assumed that the matter was considered closed by these parties. Generally speaking, we endured particularly restrictive practices in our interactions with Facebook and indeed the ODPC. Facebook's absolute refusal to accept access requests other than via their self-download tool, together with the ODPC's responses, represent restrictive practices in this case. Facebook's self-download tool has been questioned elsewhere due to its potential failure to disclose all information[72]. The complete absence of any alternative methods via which to make access requests to Facebook represents a procedural inflexibility which sits in an uneasy contrast with the sheer breadth of data collected by the company.

This appears to reflect an organisational rigidity which cannot (or does not wish to) accommodate the needs of its users and demonstrates a lack of readiness and willingness to fulfil individual subject access requests. It would be naïve to conclude from this experience that Facebook lacks the expertise and awareness of data protection matters given its status as a defining entity in the recent history of online interactions. As a result, one is forced to assume Facebook's practices in this case are a deliberate and conscious attempt to restrict citizen/user's access to their personal data. The asymmetry of power between Facebook and the individual user was acutely felt in this case and was directly illustrated by the company's short and terse responses which simply notified us of its absolute refusal to accept our request in a format other than its existing self-download tool.

The ODPC's responses meanwhile, appeared to place them firmly on the side of Facebook. Upon receipt of our complaint, they instantly declared themselves satisfied with Facebook's privacy practices and went so far as to advise that we were not legally entitled to the type of information specifically outlined in the EU Directive. Despite our raising this potential issue of (a lack of) harmonisation between Irish and European legislation, we received no direct response from the ODPC on this point. We did however subsequently receive a response from Facebook addressing the matter of automated decision making and third party data sharing specifically, almost certainly as a result of our interactions with the ODPC. Nevertheless, communications with the ODPC were somewhat fraught and it was necessary for us to re-state our legal right of access several times before receiving a response which may be deemed close to satisfactory. Unlike our interactions with the ICO in other cases, the ODPC's communication practices did not use clear and unambiguous language and indeed we did not receive any concluding correspondence from them indicating that the matter was considered closed – we simply did not hear from them again after sending an email in which we questioned their legal advice.

It appeared in this case that the success of an access request relied heavily upon the data subject's ability and willingness to pro-actively pursue the matter, and in this case in the face of repeated refusals from both the data controller and the regulator. This means that only those data subjects with the requisite resources and expertise will access the data to which they are legally entitled. Finally, it is worth noting that despite our assessment as this case as

[72] See for example www.europe-v-Facebook.org which proposes that Facebook's self-download tool offers users only 29% of the personal data held by Facebook.

being 'complete', we ultimately failed to successfully submit an access request to Facebook. Rather, while we successfully received a direct response to our third party data sharing and automated decision making queries, Facebook ultimately continued to rely upon its self-download tool as an effective mechanism to satisfy data subjects' access rights.

Google

We attempted to locate data controller contact details via the company's online privacy policy. Although some mention is made of access rights, no guidance is given on how to submit an access request and no contact details are provided for the data controller or a department/officer to whom access requests should be sent. As a result, we located an office address in London and submitted an access request to them on 05/11/13.

On 13/12/13, two days before the 40 day response limit deadline, we received an email from Google UK. The email explained that Google Inc (located in the US) is the data controller and as such we had submitted our request to the wrong office. However, we were advised that all our personal data could be accessed via Google Dashboard. They also advised that Google shares data with third parties but that they are not legally obliged to disclose the names or details of these third parties as per the Data Protection Act 1998. As such, Google directly addressed this part of our request but evidently sought to give the most restrictive answer possible whilst being legally compliant. They did not address automated decision making processes. They also did not offer to forward our request to Google Inc, advising us instead to use the Dashboard function and revisit the company's online privacy policy if we had any other queries.

We replied on 13/12/13 asking if our request was to be forwarded to Google Inc or if this was the end of the matter. We also asked for clarification on automated decision making processes and whether these are used by Google to process our data. We received no reply to this correspondence and therefore sent another email on 27/01/14 re-stating our request. On 12/02/14, we received an email from Google UK explaining that they had processed our request on behalf of Google Inc. However, this response simply directed us to use Google Dashboard once more (as well as Google Takeout, a tool we were not previously aware of). The matter of ADM processes was once again ignored.

We responded a final time the following day asking if these options were the only means to submit an access request as well as seeking clarification on the ADM issue but have received no response to date.

This case therefore demonstrated a number of restrictive practices. The ability to simply submit an access request is severely restricted by the failure to provide any contact details or an online platform via which to send such requests. Despite assuring users in their online privacy policy that 'we aim to provide you with access to your personal information'[73], there is no explanation as to how this process takes place in practice and who to contact in order to exercise this right. Having sent a somewhat speculative request to the company's London office, the reply we received was curt and simply advised us to visit our own account to find our data. Our queries were only partly answered and even then, in the narrowest term possible according to a restrictive interpretation of the law. The long delays or complete silences between communications generated frustration as did Google's refusal to address

[73] Google – Privacy Policy – Policies & Principles, available at https://www.google.co.uk/intl/en/policies/privacy/ (access 25/03/14)

parts of our request such as the matter of ADM processes. Finally, the company's constant referral to the Dashboard function of users' accounts as the only way to access one's personal data demonstrates inflexibility in their willingness to accept and process access requests in different formats, reminiscent of Facebook's repeated reliance on their self-download tool. Given that the effectiveness of such tools is unclear and as such, data subjects are left unsure whether the data presented to them in using such systems is comprehensive.

Microsoft

This case appeared to show both facilitative and restrictive practices. The privacy policy is easy and quick to locate via the organisation's website. However, the information contained within the policy is somewhat problematic and the majority of the content outlines the organisation's privacy practices in general terms. Specifically, the information regarding access rights fails to provide a detailed description of access rights or, most importantly, outline the procedural requirements of submitting an access request. The data controller is also not identified, nor a postal address provided. Instead, the content directs users to manage and correct their personal data themselves, following a number of links depending on the service to which their request relates (i.e.: Outlook, Skype, Xbox Live, etc). Should these links prove inadequate, a further link is provided to a web form to contact Microsoft.

We followed this link and submitted our request via this enquiry platform. The next day, we received a reply from Microsoft via email, asking us to verify our identity. We replied immediately simply providing the same information we had previously submitted in our initial correspondence. It is unclear why this additional exchange of emails was necessary since it did not seem to provide the data controller with any new information. Some days later, we received an email of acknowledgement, stating that Microsoft were 'currently working with our colleagues to resolve your issue'. The formulation and tone of this sentence suggested that our request was being dealt with as a complaint about the service provided by the organisation.

We subsequently received a further email from the organisation's Advocacy Manager, requesting to speak to us via telephone in order to clarify our request. Three days later, we held a telephone conversation with the Advocacy Manager during which we confirmed for the third time the nature and extent of our request.

Almost a month later, we received an email from the data controller explaining that having completed a search of their databases, the organisation 'did not find any records' of personal data concerning us which was not already available via our own account. The email did not address the issues of third party data sharing and automated decision making processes. As a result, we replied the following day asking for these issues to be addresses as well as seeking confirmation that Microsoft did not hold any personal data about us aside from the fairly basic biographical data held in our account settings.

Some weeks later, we received an email from the Advocacy Manager confirming that no personal data was held about us. The issue of automated decision making processes was addressed by stating that 'we can confirm that none of this information is used for the purposes of automated decision making in the context of Section 12 of the UK Data Protection Act 1998'. Moreover, the email directed us to browse Microsoft's privacy policy to learn about the organisation's third party data sharing practices. The privacy policy provides only general descriptions of sharing practices as well as categories of third parties with whom data may be shared.

In summary, Microsoft's practices and behaviour as part of our subject access request appeared somewhat conflicting and ambiguous. The privacy policy provides only generalised details of their data protection and privacy procedures and their access to personal data section invites users to access their own data, seemingly refusing to accept 'traditional' access requests. However, we obtained a rapid response to our web form query and, despite the exchange of several emails, eventually made contact with an Advocacy Manager who appeared to hold sufficient knowledge and expertise to treat our request with appropriate attention. However, we were surprised and suspicious by the data controller's response that no personal data was held about us. Without making an official complaint to our national DPA, there seems to be little way for us to challenge this conclusion and therein lies the systematic problem of 'unknowables'. Data subjects are at an inherent disadvantage if a data controller claims not to hold some or any personal data about them – how can data subjects challenge this if they cannot be sure themselves? If DPAs are not inclined to accept open-ended complaints from data subjects, there is little remedy against data controllers claiming not to hold personal data with data subjects unable to check this for themselves. For this reason of ambiguity and uncertainty, we consider Microsoft to have shown restrictive behaviours in this case.

CCTV

Data controller respondents frequently replied to our requests definitively stating that footage. Even when they did, obtaining our rights was often fair from straightforward. Data controller respondents frequently replied to our requests definitely stating that footage is *never* released, belying their lack of legal awareness of data protection matters. Elsewhere, data controllers in a number of cases struggled to adequately deal with the competing issues of individual access rights and third party privacy protection, causing problems and impasses to our right of access. With this in mind, even those cases assessed as showing overall facilitative practices should be viewed as frequently requiring significant efforts on our part to overcome barriers before successfully receiving our personal data.

CCTV in a metro station

This case demonstrated predominantly facilitative practices with minor exceptions. We located CCTV signage within five minutes of being on site. The visibility of the signage was adequate since it was displayed in a manner and a location which was fairly easy to find and the sign itself had a pictorial representation of a camera, rendering it easily identifiable as CCTV signage. However, the signage was the only one visible on the platform and as such cannot be described as showing exceptionally good practice insofar as alerting data subjects of the CCTV in operation.

The signage provided a telephone number for further queries. While this offers a lead for the data subject to attempt to locate the data controller, the failure to provide a postal address for the data controller places at least one additional barrier before the data subject can make a legally legitimate access request (since in the UK, requests must be made in writing). We contacted the telephone number on the signage but were directed to an automatic message explaining that this telephone number was no longer in use. An alternative number was provided. The CCTV signage was therefore out of date, and whilst an alternative number was given upon ringing the out of date contact, one may ask whether plans are afoot to replace this out of date signage.

Picture 1: Signage displaying only telephone number for contact (blanked out in picture)

We rang the second telephone number and were directed to an automatic message with several options. The first of these options was entitled 'how we use your data' and played a recorded message detailing the company's privacy-related practices. This represented one of very few instances in which data protection and privacy was directly addressed by a data controller and in this case, was offered as the *first* of several options. This demonstrates a degree of pro-active and transparent practice by the company, seemingly inviting customers to find out more about their privacy rather than effectively relegating or hiding this information behind several barriers. Having selected this option, the automatic message mentioned the Data Protection Act 1998 and described some sharing practices. It also advised data subjects to visit Transport for London's website for full details of their data protection and privacy policies.

Following this advice, we visited the company's website and located the privacy content relatively quickly. The privacy content can be located after two clicks, firstly by accessing the 'Terms and Conditions' tab at the bottom of the company's homepage. The information contained within the privacy policy is fairly basic but crucially, the webpage includes a list of specific data collection methods for further information, including both CCTV details and a section entitled 'accessing your data'. The level of detail contained in the CCTV section is excellent, detailing where CCTV cameras operate as well as how long data is stored for, who it is shared with and why CCTV systems are in operation. The 'accessing your data' section offers similarly good levels of explanation including a downloadable template via which to make subject access requests. The template's design is simple and offers an unequivocal and clear format for data subjects to make their requests, including outlining the £10 fee as well as the identification requirements. Moreover, the appendixes included with the template detailed specific contact addresses for different departments. This meant that we were able to direct our request to the department most capable of processing it, reducing delays and also ensuring that administratively inefficiency would be avoided. The template was completed and sent to the company on 4 November 2013.

On 11 November 2013 we received a confirmation email from the company, advising that our request had been received and would now be processed. The email also outlined the 40 day response time that the data controller may use before responding to our request. Subsequently, on 14 December 2013 (within the 40 day deadline), we received a covering letter and a data disc from the data controller. The letter provided significant depth on the issue of CCTV surveillance and outlined the reasons for the surveillance as well as directly addressing the two questions regarding third party data sharing and automatic decision making (by confirming that neither of these practices were used by the company in

processing our data). The letter also explained that some footage had been blurred in order to protect the privacy of other individuals captured in the footage, displaying not only an awareness of the issues surrounding disclosure of third parties' personal data but also the fact that they possess the technology to blur footage – something which other data controllers approached during this research apparently did not possess. Finally, the letter even confirmed the exact locations of the cameras which had captured the footage, a level of detail which we had not even requested.

The footage itself was easily playable. This is significant because this was the first and, to date, only instance in which a specific media programme was not necessary in order to open and play the footage. The ease and accessibility with which the data could be opened is commendable and yet another indicator of facilitative practice by this data controller. The footage was clear and of relatively good quality with all but the pictures of the data subject blurred out, ensuring the absolute protection of the privacy of other individuals captured in the footage.

The response of this data controller therefore appears to have been exemplary. Aside from the telephone number on the CCTV signage being out of date, all subsequent interactions with this data controller proved straight-forward, unambiguous and indeed very informative. The prominence of privacy as the first available option on the automated telephone menu was previously unheard of and the level of depth provided on the company's website was excellent, including specific tabs depending on the type of personal data sought (CCTV, cookies, travel cards). The provision of a template further enables the data subject to make a complete request with a single correspondence and all communications received from the data controller thereafter were timely and clear. This may lead one to classify Transport for London's response as an example of best practice in the context of this research.

However, a final sting in the tail was to come. The data subject on the CCTV footage was *not* the requester but rather an unknown member of the public. Despite having sent photo identification, full descriptions of our movement, together with timings and a description of our clothing, the CCTV footage received featured another individual who looked much like the researcher and wore similar clothing. This perhaps is a useful reminder that despite their best efforts, the demands made of data controllers when requesting this type of data can at times be difficult to fulfil. The footage was captured in a busy locale and despite photographic identification, it is not always an easy task to locate one individual on CCTV footage featuring many other members of the public. Moreover, this may also be an indication that data controllers' failures to provide complete and correct responses are not always deliberate ploys to restrict our access to personal data but rather simply the result of human error.

CCTV in open street

This case showed both facilitative and restrictive practices and locating the data controller was not straight forward initially. The CCTV in this case was operated by the local authority. Two different types of signage were found on site containing two different contact numbers. Moreover, one of the telephone numbers did not include the area code which means that, in essence, the telephone number is incomplete. The first number directed us to the Parking Enforcement team who they transferred us directly to the CCTV control room when we explained that our query was related to CCTV. In other words, they did not deal with our query in any way – this begs the question: why is their telephone number included on the

CCTV signage at all? The advice received from the CCTV control room was tentative: the respondent explained that he did not know of any procedure to request CCTV and simply advised us to send our query in writing to the CCTV control room. Incidentally, the other telephone number was for the CCTV control room itself. We were unsatisfied with this response and sought further information on the council's official website. Here, the online content was excellent and we quickly located a telephone number for the local authority's Information and Governance department which identifies itself as the organisation's data controller.

We rang this number and spoke directly to the organisation's Data Protection Officer. The knowledge and expertise of the Data Protection Officer was excellent and all steps were taken in order to avoid undue delays in processing our request.

Having sent all the required information, we received an acknowledgement email sent by the local authority once our documents were received. The email itself mentioned the 40 response deadline meaning that the local authority pro-actively took steps to ensure their own accountability. Moreover, the email quoted the relevant legislation and outlined contact details should we have any further queries. 24 days after making our first enquiry to the data controller, we received our personal data in the form of a data disc containing the relevant CCTV footage.

Overall, this was an excellent response, but only once we came into contact with the data controller. The data controller and specifically their Data Protection Officer displayed several strategies of facilitation. We were given expert advice and we were not asked why we wished to request our personal data. All necessary steps were taken in order for our request to be dealt with as quickly as possible. Receipt of our documentation was acknowledged which enabled us to track their response time against the 40 day deadline. In any case, the local authority acknowledged this deadline themselves and thus showed an approach to transparency and accountability. However, the initial difficulties in locating the data controller are notable. The CCTV signage did not contain effective contact information and indeed one of the telephone numbers was incomplete. The members of staff answering these telephone numbers lacked the required expertise to deal with a request for personal data and we were given advice which was evidently guesswork rather than the accurate, legal procedure followed by the organisation. Given the centrality of CCTV signage as a gateway for citizens to locate and make initial contact with data controllers, these are noteworthy failings. Therefore, whilst the response of the local authority once we had made our request was nothing short of exemplary, the shortcomings of the CCTV signage are also significant.

CCTV in a government building

This case showed both facilitative and restrictive practices. We quickly located the CCTV signage on site which the data controller and the purpose of the surveillance, as well as providing a telephone number for enquiries. We rang this number and the first respondent transferred us immediately to the security team upon hearing that we had an enquiry about the CCTV system. The question must immediately be asked therefore, why does the signage bear the given telephone number if the respondent cannot answer CCTV-related queries? Having been transferred to the Security Department, the manager was not available and we decided to put our query in writing to him.

We wrote to the Security Manager and submitted an official subject access request. A few days later, we received an emailed reply from the Data Access and Compliance Unit of the

national offices of the agency, located in London, which outlined that we needed to provide further information such as identification and payment. Some of the information requested (description of clothing and movements) had been provided in our previous correspondence and we therefore had to repeat ourselves. We replied to the email on and subsequently received a letter some days later from yet another source, the regional office of the agency, acknowledging our request and confirming that the process had begun. We were given a reference number and contact details for the department dealing with our request. The letter also identified the date upon which the statutory 40 day deadline would expire, demonstrating good accountability and transparency practices. Two days before the 40 day deadline, we received a letter from the regional office of the agency with our personal data with was held on a data disc.

Generally speaking, this data controller showed both good and bad practices. Some difficulties were encountered in attempting to locate the data controller. The CCTV signage, the central tool whereby organisations can inform citizens of data protection protocol, was not helpful to our attempts to locate the data controller and the contact details misdirected our enquiries to departments/individuals incapable of answering our query. However, once our request was submitted to the responsible department, the process was relatively simple thanks to the formalised internal procedure of the organisation. However, the first part of the access request process – locating the data controller – is problematic and administratively inefficient, placing the onus of locating the correct contact details heavily upon the shoulders of the data subject. An uninformed and only partially motivated citizen may have discontinued his/her request at this point.

CCTV in a bank

This case demonstrated significantly restrictive practices leading to the involvement of the DPA. We were able to locate CCTV signage immediately thanks to its positioning at eye level on several pillars throughout the branch. The content explained that CCTV monitoring was taking place as well as providing a reason for this surveillance. A telephone number was also provided for further enquiries.

On 30 May 2013, we phoned the number provided on the CCTV signage and were put through to a general customer services centre. After explaining the nature of our enquiry, we were advised that CCTV footage was usually only disclosed to the police following criminal incidents. We were also asked why we wished to request the footage. Having explained that our request was not linked to any criminal activity, the respondent placed us on hold whilst checking with her superior. After several minutes, we were advised that CCTV footage would not be released but staff at the location in which the footage was captured could review this footage on our behalf. As such, we would be required to attend the branch in person to discuss this. At this point, one may question why CCTV signage provides a telephone number for enquiries if only staff on site can actually facilitate issues of access? Data subjects are effectively being mis-directed *away* from the members of staff with the relevant procedural powers to begin the access request procedure.

We attended the branch again on 3 June 2013 and asked a member of staff for access to the CCTV footage. We were asked why we sought access to this data and replied that it was our legal right to obtain this. The bank's representative went into the back office and sought advice from an unnamed superior. Upon her return, she explained that she had spoken to her manager and had been advised that 'there is no way anyone would ever be allowed to see the

CCTV footage'. We asked her why this was the case and were told that 'this is the bank's policy'. No further advice was given.

On 12 June 2013, we wrote a lengthy complaint letter to the branch's manager, once again outlining our legal right of access under the relevant British legislation. Following this letter, on 3 July 2013, we received a telephone call from a member of the management team at the branch. During this phone call, we received an apology for the previously incorrect advice that we had been given and it was confirmed that our understanding of access rights and CCTV was correct. As a result, we were invited to attend the branch once again in order to have our identification verified, after which a request would be made to the bank's security contractor to obtain the relevant footage. As a result, on 6 July 2013, we attended the branch. During this visit, our identification was verified and we were told that the footage should be available 'very soon'.

Over a month later on 16 August 2013, we received a letter from the bank advising that '(the CCTV operators) do not have the technology to show your footage and blur the other customers in the frame. This then means that we would be breaking their Data Protection'. Several issues occur here: firstly, it is not clear why we had to wait over a month for this response, given that we had previously been advised that footage would be available 'very soon'. Secondly, the issue of blurring the footage in order to protect the privacy rights was never previously raised and it seemed uncertain (in our estimation) whether an organisation as large as the bank would be unable to employ technology to blur some material out of CCTV footage. Finally, the ICO advises data controllers to employ a balancing exercise in cases where a subject access request is made but there is a potential compromise of the privacy of third parties. The formulation of the letter we had received and the finite conclusion therein suggested to us that such a balancing exercise had not been undertaken and in fact our request had been discontinued as soon as the spectre of third party privacy issues had been raised.

Despite these reservations, we attended the branch once again on 26 September 2013 in an attempt to be captured on film with no other customers in the frame. The following day, we wrote to the bank and made a new request. On 18 October 2013, we received a response, explaining that the images had been checked and other customers did appear in shot. As a result, our request was denied. Once again, it seemed that no attempt had been made to accommodate our request and access was denied outright in order to protect the privacy of third parties.

With this in mind, we submitted a complaint to the ICO on 24 October 2013. The complaint procedure was very simple and was easily accessible via the organisation's website. The guidance notes provided were clear and we were able to submit our complaint in less than 15 minutes. Upon emailed submission of our complaint, we received an instantaneous reply via email which confirmed receipt. On 11 November 2013, we received a second email from the ICO advising that our complaint had been passed to the appropriate department within their complaint resolution but that due to a significant back-log of complaints, the response time may be lengthy.

Nevertheless, on 16 December 2013, we received a letter from the UK Data Protection and Compliance department of the bank. The letter explained that following consultation with the ICO, our complaint had been reviewed and we received an apology for the problems we had encountered. We were also advised that the CCTV footage we had requested would be re-

instated and would be made available to us as soon as possible. In order to begin this process, we were asked to confirm once more the date of the relevant footage. We replied on 18 December 2013 with confirmation of the date of the footage.

On 18 December 2013, we also received an email from the ICO with a full explanation of their decision in this case. It was outlined that our complaint had been upheld and that the bank were now taking remedial action to fulfil our request retrospectively. Regarding taking further action against the data controller, the email explained:

> 'Based on the information provided in relation to this complaint, the Commissioner has decided that further regulatory action is not required at this time. When deciding whether regulatory action is appropriate, we take into account the organisation's general record of compliance with the DPA. This may include any previous assessments we have made, or any regulatory action we have already taken against the organisation.'

The email was clear and explained in intelligible terms the actions and decisions taken by the ICO in resolving our complaint.

On 24 December 2013, we received confirmation from the bank's UK Data Protection and Compliance department that they were undertaking a search for the relevant CCTV footage and once available, we would be contacted in order to collect this data in person from the branch. On 20 January 2014, we received this confirmation and were invited to collect the data.

On 24 January 2014, we attended the branch and collected the data once our identification was verified. The data disc was accompanied with a detailed step-by-step guide explaining how to open data files using the organisation's internal CCTV viewing programme. The footage itself was relatively clear and included several different angles captured by five CCTV cameras. The faces of other customers in the branch were blurred out although this was done somewhat crudely, perhaps indicating that the technology required to do this was not available but a work-around solution was found in order to fulfil this requirement.

In summary, whilst our request was ultimately satisfied, the process in order to obtain our personal data was lengthy, complicated and generally dissatisfactory. Over six months passed between making first contact with the data controller to receiving our personal data. During the course of these six months, we were required to telephone the organisation twice, write to them four times and attend the branch in person five times. We were also required to make a complaint to the ICO after being denied access to the footage on two separate occasions. The crux of the breakdown of the access request procedure in this case appeared to be a lack of understanding and knowledge of data protection and privacy issues by members of the organisation. After being denied access outright, a member of the management team acknowledged the bank's error and sought to fulfil our request. However, when the ambiguous matter of third party privacy compromise occurred, our request was once again flatly denied. It was not until a member of the organisation's data protection department became involved (following our ICO complaint) that the validity of our request was recognised and access to our personal data was finally facilitated. Lack of procedural expertise therefore thwarted our access request at more than one interval. However, this ultimately successful outcome was achieved by ongoing and (somewhat) relentless communications with the data controller, culminating in a complaint to the ICO. One must therefore question whether all data subjects would partake in such a time and resource

consuming exercise or if, in another case, the administrative incompetence of the data controller would have resulted in the data subject simply abandoning the request.

Finally, this case does enable us to make one positive finding: the ICO's intervention was not only timely but ultimately led to a successful outcome. Communications with the ICO were prompt at all times as well as being very clear, providing those data subjects with little or no data protection/privacy expertise with unambiguous guidance on the subject access request process and one of the avenues for redress (i.e.: making a complaint) in cases where access is denied.

CCTV in department store

While this case showed some instances of facilitative procedures, severe restrictive practices were also evident. In searching for CCTV signage on site, we located a 'reflective' screen at the entrance of the store, showing a live CCTV feed of customers as they enter the store. This is intended, we presume, to act as reassurance for customers together with alerting them of the presence of CCTV surveillance. Despite walking throughout the store and spotting numerous CCTV cameras, we did not find a single CCTV sign. Given the number of cameras and the reputation of the company itself (as a high-end retailer), we were surprised by such an elementary error in data protection and privacy procedure. We asked a member of staff for guidance but were met with confusion and a sense of amusement at our request, as though a question about CCTV was farcical rather than one to be treated with proper care and attention. We were advised that the respondent 'would imagine there are some near the doors' but she did not accompany us to check. In fact there were no signs whatsoever, despite other signage being prominent on other parts of the store including opening/closing times and a sign indicating accepted methods of payment in the store.

With this inability to locate any signage (and thus any data controller contact details) in person, we visited the organisation's official website. The privacy policy can be quickly located with a single click with the privacy link located at the bottom of the webpage. The policy itself is reasonably extensive and explains the type of data collected by the company, how this data is stored and who it may be shared with. However, the policy makes no mention specifically of how a citizen may access data and fails to explain the process of subject access requests. Whether this omission is deliberate or not is impossible to say but the complete failure to mention data access is poor practice given that the rest of the information provided is reasonably thorough. Nevertheless, the data controller for the company is identified and an address is given for privacy-related queries. The usefulness of this identification is questionable in light of the failure to outline data access rights: a lay citizen with little knowledge of data protection matters may visit the website and simply assume that he/she has no right to request access to data since this is completely ignored in the company's privacy policy.

Using the address provided, we sent a subject access letter on 12/11/13 without identification or a fee since these requirements were not mentioned in the privacy policy. On 19/12/13 we received an email from the company's legal department in London asking for the £10 fee as well as identification. Had this been outlined in the privacy policy of course, we would have been able to send this in our first correspondence. The failure to do so meant that we were obliged to send two separate letters at the detriment of time and money. The email did however mention that once the fee and identification had been received, the company would have 40 days in which to respond to our request. The disclosure of their statutory response

time demonstrated transparency and accountability as well as effective management of customer expectations. We responded to the email the same day and sent the requested documentation on 12/11/13.

On 20/11/13 we received another email from the same source acknowledging receipt of our payment and identification and quoting 29/12/13 as the day on which the 40 day deadline would expire. Once again, the provision of a fixed date demonstrated a commitment to effective transparency and offered the customer/citizen a clear indication of when we should expect to receive a response. Shortly thereafter on 25/11/13, we received a letter from the company's Executive Office stating that our request had been passed to the relevant data protection officer. The timing of this letter seemed a little tardy given that we had been dealing with the DPO for over two weeks by this point. We assumed this letter had been sent either in error or with some delay which, whilst showing some administrative oversight, was nothing to be concerned about.

On 05/12/13 we received a letter and data disc containing our personal data. Given that we had been quoted 29/12/13 as the expiry of the 40 day deadline, the receipt of our personal data by 05/12/13 showed that the company were able to fulfil our request well ahead of their permitted timeline. The covering letter explained that the company did not believe CCTV footage to be our personal data since the Data Protection Act 1998 proscribes that personal data must have 'the data subject as its focus'. Since the CCTV cameras in the store were fixed and recorded all customers rather than specifically just us and did not 'follow' us around the store, they believed that this did not constitute personal data. Nevertheless, they outlined that they were still willing to disclose the CCTV footage we had requested and enclosed a data disc containing this data.

This reading of the DPA 1998's provisions with regard to fixed CCTV cameras is unique in all correspondences we have received with CCTV-based data controllers. Even in cases where access has been refused, this reason had not previously been given. In our opinion, the company's reading of the legislation is incorrect and the ICO has previously outlined that sophisticated CCTV systems (i.e.: systems that go beyond one or two fixed cameras such as those in a small store) are indeed subject to the provisions of the DPA 1998 and of the Section 7 data access requirements.

The letter also addressed the issue of third party privacy by asking us to be mindful of this matter since third parties are not blurred out of the footage and that the company are disclosing the footage to us on the basis that the footage is treated confidentially. This approach demonstrates that the company undertook a balancing exercise, considering our right of access against third parties' right of privacy which is the procedure recommended by the ICO. As a result, the company demonstrated an awareness of their data protection and privacy responsibilities to both the requester and to third parties affected by the request.

The footage itself was somewhat grainy and frequently cut to a blank screen for long periods of time when switching from one camera feed to the other. The data disc contained a program on which we were able to view the footage but it took us a long time to figure out how to work this program since the letter enclosed provided no guidance about this whatsoever. If we were not familiar with similar programs as a result of this research, we would likely have been unable to view the footage. There is therefore an issue here in terms of the data controller's legal duty to communicate our personal data in a format which is intelligible. The

failure to explain how to work the CCTV viewing program potentially infringes this requirement.

The letter received also failed to answer our query regarding automated decision making processes which may be utilised in CCTV systems via facial or gait recognition software. Given this omission, we emailed the data controller on 5 December 2013 asking for clarification on this matter. On 16 December 2013, we received a response explaining that the data controller was 'unable to give you details of the systems operated'. Following another email exchange, we were advised that this refusal to answer was because the company did not believe we were entitled to this information under the Data Protection Act 1998 and that 'as a business, we prefer not to disclose (details of our system)'. As a result, we sent a further email on 7 January 2014, quoting from the Data Protection Act 1998 and arguing that we were entitled to know if automated decision making processes had been used in processing our data. On 8 January 2014, we received a response stating that 'no automated decisions which would fall into Section 7(1)(d) have been made about or regarding you and therefore we have no further information to provide to you'. The fact that this simple disclosure necessitated three separate email exchanges demonstrated the apparent reluctance by this data controller to reveal any information beyond the bare minimum level of disclosure to data subjects. Moreover, obtaining this information required sustained and numerous attempts, once again demonstrating that only those individuals with time, knowledge and effort can expect to successfully receive complete responses to their requests.

In summary, this case showed examples of both facilitative and restrictive practice in this case. The complete absence of CCTV signage in the store was an exceptionally poor and indeed unlawful practice according to British law. This instantly restricts the data subject's ability to request his/her data as a natural 'lead' to follow is not given. The member of staff's evident indifference to our query about this further exacerbated the poor data protection practice displayed here. The online content was adequate but the glaring omission of any mention of access rights once again fundamentally undermined citizens' ability to exercise their rights. While a contact address was given, the failure to give any other information regarding accessing one's data arguably undermines the remainder of the reasonably good content in the company's online privacy policy. The lack of information regarding access requests, such as fee and identification requirements, was compounded when it was necessary for us to send payment and ID in a separate, second correspondence.

However, once we had submitted a subject access request together with the fee and ID, the company's practices improved immeasurably. We received regular and clear communications from the company's legal officer and were given a fixed date by which we should expect our request to have been dealt with. We received our personal data in a timely manner and well in advance of the expiry of the 40 day deadline.

Perhaps this case best illustrates the problem with making subject access requests in the UK. Once the request is made and is complete (in terms of providing payment and identification), a clear procedure emerges to accept and process access requests. However, the problem lies at the point before a request is made. Data controller practices are restrictive and deny the citizen information on firstly how to make a request and secondly who to contact in order to do so. The absence of CCTV signage failed to advise citizens not only of the presence of CCTV surveillance but also of who controlled this system. The lack of online information concerning access rights means that citizens are required to pro-actively dig out this information, potentially be submitting questions to the company resulting in a long-winded,

costly and lengthy process of sending correspondences back and forth which could be avoided if all necessary information was openly provided by the data controller in the first place. Alternatively, the citizen must be aware of his access rights before approaching the company but this assumes a greater level of data protection expertise amongst citizens than is realistically the case. In either scenario, the onus is always upon the citizen to take the lead in activating his/her right of access to the extent that this burden is, in our opinion, disproportionate.

CCTV in a stadium

This case generally displayed restrictive practices although it is also an example of the potential for administrative error in the failure to obtain personal data. While attending the site, we located CCTV signage after approximately 15 minutes despite walking through several sections of the stadium. The signage identified 'The Football Trust' as the body responsible for the operation of the CCTV but provided no contact details. As a result, we searched online for this body but could not locate an official website. A brief entry in Wikipedia explained that this body was replaced in 2000 by the Football Foundation, effectively meaning that the CCTV signage details identifying The Football Trust as the data controller were at least 13 years out of date.

We visited the Football Foundation's website and quickly located the privacy policy. The privacy content therein was reasonable strong and provided a postal address for privacy related queries. As a result, we submitted a subject access request to this address on 02/12/13. On 10/12/13, we received an email from the Football Foundation explaining that they were not in fact the data controller for the CCTV but may possibly have been identified on the signage because they had in the past provided some funding for such systems. Instead, we were provided with an email address for an officer at the football club who we were advised to forward our request to. We did so on 10/12/13. Thereafter, we received no reply for several weeks. On 27/01/14, we sent another email to which we again received no reply.

As a result of the lack of response received, we submitted an official complaint to the ICO on 24/02/14. Shortly thereafter on 05/03/14, we received a response from the ICO explaining that they had advised the football club that they should reply to our request as soon as possible and in any case within 21 days.

On 10/03/14, we received an email from an officer at the fooball club identifying himself as the club's data controller. In his email, he explained that the email address we had been contacting was spelled incorrectly and as a result the emails were never received, hence the club's non-response. He further advised that due to the time delay in our request finally reaching him, the footage had since been erased. He did however, after some further exchange in emails, confirm that the CCTV system did not operate any automated decision making processes. He did not address the issue of third party sharing practices.

In summary, the failure to obtain our personal data in this case may be attributed to the administrative/human error of the mis-spelt email address. We were provided this address by The Football Foundation but it seems that although this was incorrect, it was nevertheless given in good faith. However, a noteworthy failure remains in the significantly out of date signage displayed by the club. The identification of The Football Trust as the data controller renders the sign at least 13 years out of date and had we in fact been given the correct email address, there is a high likelihood that the delay incurred by mistakenly submitting our

request to The Football Trust may have jeopardised our request even if we had been given the correct email address in any case.

Concluding thoughts

Our experience of attempting to submit subject access requests has illustrated a range of facilitative and restrictive practices on behalf of data controllers. Little systematic trends were observed between public and private organisations with data controllers from both sectors displaying varying levels of facilitation/denial of our requests during this research.

Third Party Data Sharing and Automatic Decision Making Processes

Data controllers dealt with these questions in vastly different ways, from addressing them openly and directly to ignoring them and refusing to engage with us any further. However, it should be noted that, to date, not a single data controller responded by addressing these matters without further prompting from us. As a result therefore, even in cases where these questions were eventually answered to our satisfaction, the onus was placed on the citizen to ensure that the data controller did not ignore this aspect of the request.

At the facilitative and transparent end of the spectrum, data controller responses answered these questions directly, although this necessitated varying amounts of prompting from us. As explained above, in the case of the mobile phone carrier we were advised that automatic decision processes are not used and their data sharing policy was disclosed in general terms.

Other data controllers appeared to answer queries regarding third party data sharing and ADM processes only selectively. The vehicle licensing agency, for example, showed transparent practices by directly addressing the issue of third party data sharing without any prompting from us. Firstly, they explained their policy in general terms and, secondly, they provided a specific example of having shared our data with the police in connection with a speeding offence three years previously. However, the matter of automatic decision making processes was not addressed at all and repeated attempts to contact the agency thereafter have been unsuccessful to date.

In a number of other cases (for example in the sites of banking records and loyalty card with a supermarket), data controllers readily disclosed our personal data and appeared to practice facilitative procedures by employing open lines of communication with us, responding to our requests in a timely manner. However, these responses completely ignored our queries regarding third party data sharing and automatic decision making processes. Once we contacted these data controllers again, asking them to directly address these two matters, the previously open communication strategy suddenly appeared to dry up. While we finally received a reply from the supermarket on this matter, this was almost three months in coming. Meanwhile, we never received any response from the bank and our query remains unanswered to date.

The mixed responses from data controllers regarding the matters of third party data sharing and automatic decision making processes evidenced both facilitative and restrictive strategies. While some respondents at least attempted to address these matters, others required repeated prompting from us before finally answering our questions. Worse still, some data controllers, despite disclosing what personal data they held about us with relative openness, completely ignored these additional parts of our requests and seemingly refused to enter into any further dialogue with us as we attempted to seek answers to these questions.

The role of DPAs and redress mechanisms

Two DPAs were encountered as part of this research – the Information Commissioner's Office (UK) and the Office of the Data Protection Commissioner (Ireland). As the relevant cases above show, our experiences with these organisations differed greatly. The case in which the ICO was involved was resolved successfully and the regulator helped us to overturn an unjust denial of our access rights. Moreover, we enjoyed clear communications with the ICO, culminating in an email to which was attached a concluding statement which not only outlined the steps taken as part of the case but also officially closed the matter, successfully 'closing the loop' on the case in question.

In contrast, our communications with the ODPC were difficult and the regulator appeared to immediately place itself in direct opposition to us by unequivocally backing the data controller in the case (Facebook). As our correspondences progressed, we were required to employ our data protection expertise and even highlighted a potential conflict between national and European law. We had no further communications with the ODPC thereafter but this exchange of emails did at least appear to prompt Facebook into responding to our request in more detail.

More generally, we often experienced an asymmetry of power in our interactions with some data controllers. The problem of 'unknowables' which occurred as part of our request to Microsoft left us with the impression that unless a flagrant or more tangible breach of data protection principles has occurred, the data subject may be left with no effective redress mechanisms. This feeling was compounded as part of requests made to CCTV data controllers who claimed that our footage had been destroyed. While a complaint to a DPA may have led to some action against the data controller, we would nevertheless ultimately be left with an unfulfilled request. The solution to such a problem is not easy but one possible remedy would be for CCTV data controller to ensure that they respond to CCTV data requests with great haste in order to avoid undue delays which may (and in the case of this research, did) lead to footage being lost.

Facilitative practices

Several data controllers did however display facilitative approaches. These cases generally involved the availability of access request templates which made clear the requirements of a request and ensured that citizens are able to avoid undue delays in the processing of their requests. Many data controllers also pro-actively outlined the time requirements to which their responses were subject, demonstrating an admirable level of self-regulation as well as good administrative procedure. A limited amount of exceptional cases involved the disclosure of personal data which was not only extensive but was also delivered in a timely fashion and processed in a professional, exemplary manner.

SIGNIFICANCE OF FINDINGS – UNITED KINGDOM

A number of key findings have emerged during the course of the research. From a legal perspective, the development of case law in the UK in the field of access rights has led to narrow interpretations of key data protection and privacy definitions. This includes concepts such as 'personal data' and case law has shown that data subjects may encounter significant obstacles in exercising their access rights. The empirical phase of the research also illustrated a number of findings, as detailed below.

Negative/Restrictive communication strategies

During direct interactions with data controller representatives either on the telephone or face to face, we often experienced the use of negative language and demeanour which was manifested by suspicion, scepticism and impatience. Telephone conversations were at times punctuated by long silences, audible sighs, requests to repeat our questions several times and, in one case, patronising advice to 'go away and think about this more carefully'. Whilst difficult to capture systematically and scientifically, these communicative practices created conversations and interactions which instantaneously placed the requester and the data controller in oppositional and conflicting roles. Such situations meant that it was necessary for us to forcibly assert our rights but this, of course, is not the kind of process that all citizens may be comfortable undergoing. The right of access therefore appears to be one which is exercisable only by those confident enough to enter into (at times) difficult negotiations with representatives who ought, in theory, to facilitate our requests rather than attempt to deny them.

Administrative/procedural inefficiency

At other times, denial strategies could only be viewed as deliberate or negligent. Several data controllers provided us with templates via which to make access requests only *after* we had already sent a first correspondence. Similarly, we were often asked to send identification and payment in an additional correspondence simply because the data controller had not made these requirements clear in their privacy policies. These approaches invariably mean that the citizen's request is not only delayed (a potentially very significant matter in cases of CCTV footage) but that citizens will often incur additional postage costs due to being asked to send more than a single letter in order to make a complete request. There is no obvious reason, in our opinion, why templates (if data controllers insist on using them) are not made openly available to requesters on organisations' websites.

A number of data controllers in this research also failed to answer our requests fully, often ignoring our questions concerning third party data sharing and the use of automated decision making processes (as outlined above). In these cases, we were required to contact the data controller once again (several times in some cases) before finally receiving a complete response. As a result, similar issues of time and cost were incurred, demonstrating the tangible effects of data controllers' poor practices.

In both instances, the burden of cost and time is placed on the data subject. As with the discussion of the (lack of) data protection expertise, the requester is expected to pro-actively pursue matters and incur cost and time penalties as a direct result of administrative and procedural incompetence in behalf of data controllers.

Lack of knowledge and expertise

Many data controllers and their representatives lacked the knowledge and awareness to answer our queries accurately, often dismissing our requests altogether or directing us down blind alleys. These strategies of denial can be viewed as unwitting since the advice, whilst being incorrect and/or incomplete, is generally given in good faith. However, although this can be viewed as unwitting on an individual level, from the perspective of the organisation, it may be argued that the failure to adequately train members of staff on data protection matters is a wilful strategy of denial. This often meant that in order to successfully receive our personal data, we were required to effectively educate several data controller representatives about data protection legislation and our legal right of access. This necessitated ongoing negotiation processes and perseverance on our behalf in order to overcome the barriers erected due to the endemic lack of data protection awareness. As a result, the burden of successfully obtaining personal data was systematically placed upon our shoulders. So while we managed to enact our rights in seven out of ten cases, we suspect that this is a consierable over estimation of ordinary citizens' experiences. This was not an insurmountable obstacle given our status as data protection researchers but one can speculate that those data subjects with limited expertise in such matters are likely to have discontinued a number of the above (ultimately successful) cases as a direct result of being given incorrect advice. As such, access to personal data is effectively restricted to those requesters with extensive knowledge of the process and the legalities around data protection matters.

The problem of 'operationalisation'

In many cases, once requests were submitted, minor issues aside, we were often able to obtain our personal data relatively straight-forwardly (but not necessarily information on data sharing or ADM processes). However, the fundamental issue lies in the crucial juncture of the dynamics of the submission process between locating a data controller and actually submitting a request. In other words, 'operationalising' our access rights. Perhaps the best example of this juxtaposition in this research came in the example of CCTV in a department store, where the complete absence of signage together with the lack of knowledge of staff members rendered our attempts to locate contact details for the data controller very difficult. However, once the access request was finally successfully submitted, a dedicated officer within the organisation processed our request with the upmost professionalism and compliance with data protection legislation.

The complete (or near-complete) absence of CCTV signage in some cases, coupled with little or no information on organisations' online privacy policies, severely restricted our attempts to make subject access requests. Elsewhere, the advice received from data controller representatives often discouraged us from making a request and it is a fair assumption to make that a 'lay person' lacking some knowledge of data protection and access request procedures may have been inclined to discontinue their attempts to access their personal data. A number of respondents expressed surprise during this research at the nature of our requests and explained that our request was the first of its kind that they had received. One must consider why this is so and in many cases, the strategies, approaches and procedures employed by organisations inherently discourage citizens from exercising their right of access. Data subjects seem to be expected to hold significant knowledge of their access rights in order to be able to exercise them. This is a peculiar paradox given that one of the central tenets of informational rights is to enable citizens to inform themselves about how to manage and protect their personal data. The right of access seems to have become a right one can only exercise successfully if one has a high level of knowledge of data protection and privacy law

together with the requisite time and resources in order to break through the series of barriers created by the (deliberate or otherwise) strategies of denial employed by data controllers.

References

Amberhawk (2012) An Analysis of Google's Privacy Policy and Related FAQs http://www.amberhawk.com/uploads/Google_privacy_docs.pdf (Accessed 19 May 2013)

Chalton, S. (2004) 'The Court of Appeal's interpretation of "personal data" in Durant v FSA – a welcome clarification, or a cat amongst the data protection pigeons?', *Computer Law and Security Report*, 20(3): 175-181

Durant v Financial Services Authority [2003] EWCA Civ 1746

Edwards, L. (2004) 'Taking the "personal" out of personal data: Durant v FSA and its impact on the legal regulation of CCTV', *Script-ed*, 1(2): 342-349

Espiner, T. (2013) 'Police number plate camera scheme broke law in Royston', *BBC News*, http://www.bbc.co.uk/news/technology-23433138 (Accessed 24 July 2013)

Europe v Facebook (2013) 'Get Your Data – Make an access request at Facebook' http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html Accessed 19 May 2013

European Union (1995) 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data' http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (Accessed 15 March 2013)

European Union (2007) 'Article 29 Data Protection Working Party – WP136: Opinion 4/2007 on the concept of personal data' http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (Accessed 10 January 2014)

Ezsias v Welsh Ministers [2007] All ER (D) 65 (Dec)

Google (2014) 'Privacy Policy', https://www.google.co.uk/intl/en/policies/privacy/ (Accessed 14 February 2014)

Home Office (2013) 'Surveillance Camera Code of Practice' https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf (Accessed 1 July 2013).

Information Commissioner's Office (2008) CCTV Code of Practice http://www.ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx Accessed 19 May 2013

Information Commissioner's Office (2012) 'Draft Subject Access Code of Conduct' http://www.ico.gov.uk/about_us/consultations/~/media/documents/library/Corporate/Researc

h_and_reports/draft_subject_access_cop_for_consultation.ashx (Accessed 19 December 2012).

Information Commissioner's Office (2013a) 'Find out how to access your personal information' http://www.ico.gov.uk/for_the_public/personal_information.aspx (Accessed 19 December 2012).

Information Commissioner's Office (2013b) 'Register of data controllers' http://www.ico.org.uk/what_we_cover/register_of_data_controllers (Accessed 6 August 2013).

Information Commissioner's Office (2013c) 'Information Commissioner's Annual Report and Financial Statements 2012/13' (http://ico.org.uk/about_us/performance/~/media/documents/library/Corporate/Research_and_reports/ico-annual-report-201213.ashx (Accessed 26 March 2013).

Information Commissioner's Office (2013d) 'Data Protection Act 1998 – Supervisory Powers of the Information Commissioner – Enforcement Notice – Dated 15 July 2013' http://www.ico.org.uk/~/media/documents/library/Data_Protection/Notices/hertfordshire-constabulary-enforcement-notice.pdf (Accessed 6 August 2013).

Information Commissioner's Office (2014) 'Enforcement performance', http://ico.org.uk/about_us/performance/enforcement_performance (Accessed 26 March 2014)

Jagessar, U. and Sedgwick, V. (2005) 'When is personal data not "personal data" – The impact of Durant v FSA', *Computer Law and Security Report*, 21(6): 505-511

Johnson v Medical Defence Union [2007] EWCA Civ 262

Lorber, S. (2004) 'Data Protection and Subject Access Requests', *Industrial Law Journal*, 33(2): 179-190

Maude, F (2012) 'GOV.UK – The start of a new way of delivering public services', *Cabinet Office*, available at http://digital.cabinetoffice.gov.uk/2012/10/16/gov-uk-the-start/ (Accessed 12 June 2013)

McCahill, M., and C. Norris (2002) 'CCTV in Britain' *Urban Eye Project, Working Paper No. 3.* http://www.urbaneye.net/results/ue_wp3.pdf Accessed 12 June 2013

PRESCIENT (2012) Deliverable 3 – Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data http://www.amberhawk.com/uploads/Google_privacy_docs.pdf Accessed 19 May 2013

Rempell, S. (2006) 'Privacy, personal data and subject access rights in the European Data Directive and implementing UK statute: Durant v Financial Service Authority as a paradigm of data protection nuances and emerging dilemmas', *Florida Journal of International Law*, 18: 807-842

Smith v Lloyds Bank TSB plc [2005] EWHC 246 (Ch)

The Data Protection (Miscellaneous Subject Access Provisions) Order (2000) http://www.legislation.gov.uk/uksi/2000/419/contents/made (Accessed 30 May 2013).

The Data Protection Act (1998) http://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed 31 March 2013)

Wotherspoon, K. (2003) 'Access Denied – Court of Appeal rules on subject access requests', *Privacy Laws & Business*, 14: 1-3

List of Abbreviations

ACPO – Association of Chief Police Officers

ADM – Automated Decision Making

ANPR – Automatic Number Plate Recognision

CCTV – Closed Circuit Television

DPA – Data Protection Authority

DPA 1998 – Data Protection Act 1998

DPO – Data Protection Officer

FAQ – Frequently Asked Questions

ICO – Information Commissioner's Office

MDU – Medical Defence Union

NGO – Non-governmental Organisation

ODPC – Office of the Data Protection Commissioner

PNC – Police National Computer

PNR – Passenger Name Record