Exercising Access Rights in Europe

Professor Clive Norris & Dr Xavier L'Hoiry
University of Sheffield
IRISS Sheffield Workshop
24-25 June 2014

Overview of the project

- 10 partner institutions
- Project divided into three key parts
  - Analysis of legal frameworks of access rights
  - Locating data controllers
    - 327 sites visited
    - Measured ease of locating data controller contact details online, in person and via telephone.
  - Submitting access requests
    - 184 individual requests submitted
    - Asked data controllers to disclose personal data and provide information regarding data sharing & automated decision making.

Headline Findings

- 20% of data controllers cannot be identified before submitting an access request
- 1 in 5 CCTV operators do not display any signage.
- 43% of requests did not obtain access to personal data.
- 56% of requests could not get adequate information regarding third party data sharing
- 71% of requests did not get adequate information regarding automated decision making processes
- Subversion of the law – law in books vs. law in action

Discourses of Denial

- Data controllers employ several key discourses of denial which restrict data subjects' ability to exercise their rights.
  - Out of Sight
  - Out of Court
  - Out of Order
  - Out of Time
  - Out of Tune
  - Out of Mind

Out of Sight

- Data controllers render themselves 'invisible', severely restricting and delaying the access request process.
  - Silence in response to requests
  - Poor content in privacy policies
  - Inability to identify single officer to liaise with within an organisation
  - Lack of/poor CCTV signage

Out of Sight (cont.)

Out of Court

- Data controllers and their representatives incorrectly rely on legal exemptions to rule requests 'out of court'.
  - *'Only the police may have access to CCTV footage'*
  - *'You don't have a right to see the data but only a list of what data is held about you'*
  - *'You cannot view the footage because it would infringe the privacy of others'*
  - *'As you are not a customer, you do not fulfil the category of 'personal' according to data protection law'*
  - *'It would be illegal to share such data with a citizen'*
  - *'We would never disclose such data'*
- The requirement of 'justifying' requests

Out of Time

- Time is used in a variety of ways to restrict and delay access requests.
  - Data controllers respond beyond legal timelines.
  - Lengthy delays before receiving disclosure of personal data.
  - Data retention periods used as a shield to avoid disclosing data (i.e.: CCTV footage).

Out of Order

- Data controllers' own administrative and bureaucratic procedures are inadequate and the access request process therefore breaks down.
  - Technical problems
  - Missing information in disclosure of personal data
  - Missing/lost letters to and from data controllers
  - Outdated information on privacy notices
  - 'Dead' telephone numbers
- Not an exhaustive list!

Out of Tune

- Some data controllers only accept requests using extremely narrow mechanisms, therefore restricting ability to exercising informational self-determination.
  - Linguistic imperialism
  - Self-download tools
  - Knowing the unknowable

Out of Mind

- In a minority of cases, data controllers' reactions to access requests give the data subject the feeling that they are 'out of their minds' for making such a request.
  - Abuse of democratic rights
  - Nefarious motives
  - Suspicion and passive aggression

Reflections on data protection law

- Circumscription of the law
- Inconsistency of implementation into national law
  - Uncertainty for citizens
- Law subverts itself
  - 'Motivating' requests for CCTV data
  - Third party data sharing – 'categories of recipients'
  - Legal definition of automated decision making
- Law in books vs. law in action

Policy Recommendations

- It should not be necessary to 'motivate' requests.
- Data controllers must render themselves more 'visible'.
- Organisations should have a recognised officer tasked with dealing with access requests.
- Data controllers should be required to disclose *specific* information about data processing (i.e.: data sharing & automated decision making)
- Data Protection Authorities should be empowered to raise data protection awareness and carry out audits of data controllers.

Best Practices

- All is not lost!
- Several examples of facilitative practices experienced during the research
  - Clear and helpful CCTV signage
  - Detailed privacy policies
  - Provision of templates
  - Unambiguous access request administrative procedure
  - Transparent data collection and storage practices
  - Timely responses
  - Thorough disclosure of personal data

Conclusion

- What do data subjects need to successfully submit an access request?
  - A law degree
  - Fluency in English
  - Confidence
  - Extensive knowledge of data protection law
  - Resilience