The Sedona Conference Journal

Volume 16 2015

The Citizen and the Litigant—Balancing Interests in the Digital Age

Quentin Archer

Recommended Citation:

Quentin Archer, The Citizen and the Litigant—Balancing Interests in the Digital Age, 16 Sedona Conf. J. 311(2015).

For this and additional publications see: https://thesedonaconference.org/publications

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual basis, containing selections from the preceding year's conferences and Working Group efforts. The Journal is available on a complementary basis to courthouses and public law libraries and by subscription to others ($95; $45 for conference participants and Working Group members). Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. Check our website for further information about our conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference at comments@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® designed by MargoBDesignLLC
See margobdesign.com or mbraman@sedona.net.

Cite items in this volume to "16 Sedona Conf. J. _____ (2015)."

THE CITIZEN AND THE LITIGANT—BALANCING INTERESTS IN THE DIGITAL AGE

*Quentin Archer**
Hogan Lovells International LLP
London, UK

INTRODUCTION

Although data protection legislation in some form has been in existence for up to 40 years, and has covered the European Union (EU) for almost 20, EU citizens are now the subject of the most extensive and intrusive data usage techniques ever deployed. Many companies operate on the fringes of the law, rarely courting attention because their activities are not widely known, providing services which enable individuals to be analysed and targeted for a wide variety of products, usually without their knowledge. Governments of many types have engaged extensively in surveillance activities, ostensibly for crime prevention purposes. Journalists have obtained data in dubious circumstances in order to generate stories of questionable public interest.

The position is not markedly better for individuals whose data is caught up in litigation. The fact that almost all documents in litigation nowadays are already in digital form means that they can be reviewed, transferred, and analysed much more

* Quentin Archer is a Consultant with Hogan Lovells International LLP in London. He is a Solicitor of the Senior Courts of England and Wales with over 30 years' experience of advising on the resolution of international disputes, both in the UK and in other jurisdictions. Since 1984 he has also regularly advised on obligations arising out of UK and European data protection legislation.

freely and easily than was possible before. Casual comments and incautious statements are preserved for years to the embarrassment of the author of the email or instant message in which they were contained. Law enforcement authorities can gain access more easily to material which may encourage them to commence proceedings against people who in earlier days may never have come to their notice.

Documents containing personal data which are processed for the purposes of litigation in the EU, or by EU data controllers, will be subject to EU data protection rules. Because of the broad interpretation of the concept of personal data,[1] and the fact that most documents are nowadays processed in electronic form, data protection law will affect all litigation involving EU-based parties.

However, despite the pervasive application of data protection law, there is very little guidance available concerning its practical application in the context of litigation. This article examines certain aspects of the effect of EU data protection rules on documents held for the purposes of litigation and suggests: (a) how existing rules may affect the processing of such documents and (b) what changes might be made to current practices in order to ensure a fair balance between the interests of litigants in achieving a just result and the interests of individuals in maintaining their privacy.

THE NEW EU DATA PROTECTION REGULATION

For well over three years, a draft EU Data Protection Regulation ("Regulation") has been under discussion. There continues to be considerable debate about its form and content, but it

1. *See, e.g.*, *Opinion 4/2007 of the Article 29 Working Party on the 'Concept of Personal Data*,' WP 136 (June 20, 2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

is generally agreed that the fundamental principles of data protection law should not change. Instead, the challenge is how best to achieve full harmonisation throughout the EU and how the principles should be applied in practice to rapidly evolving data usage techniques.

The draft Regulation has been the subject of an enormous amount of proposals for change. The draft approved by the European Parliament in March 2014 (unfortunately not published officially in a consolidated version, although unofficial consolidations exist) differed markedly from the original of January 2012.[2] There were further, extensive differences in the draft approved by the Council of the European Union on 15 June 2015.[3] Like the current EU Data Protection Directive,[4] however, it does not expressly deal with the processing of personal data in the context of litigation. Instead, the expectation is that all processing of personal data, in whatever context, will be subject to the general principles set out in the Regulation.

---

2. *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (January 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

3. Council of the European Union, Interinstitutional File 2012/0011 (COD), document 9565/15 (June 11, 2015), *available at* http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf [hereinafter Document 9565/15].

4. 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, 1995 O.J. (L 281) 31-50 [hereinafter Data Protection Directive].

When introducing the first published draft of the Regulation in January 2012, the European Commission announced[5] that:

> [t]he proposed changes will give you more control over your personal data, make it easier to access, and improve the quality of information you get about what happens to your data once you decide to share it. These proposals are designed to make sure that your personal information is protected—no matter where it is sent or stored—even outside the EU, as may often be the case on the Internet.

Quite how this could apply to litigation, where the individual typically has no real control over the use of his or her data, is not at all clear.

THE ARTICLE 29 WORKING PARTY'S WORKING DOCUMENT

The Article 29 Working Party established under the EU Data Protection Directive considered the processing of data in the context of litigation in its Working Document 1/2009 on Pre-Trial Discovery for Cross-Border Civil Litigation ("Working Document").[6] The Working Document referred several times to the work of the Sedona Conference. The Article 29 Working Party did not issue a full Opinion on the subject, because, in its words, "these matters can only be resolved on a global basis,

5. European Commission Fact Sheet, "*Why do we need an EU data protection reform*?" (January 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf.

6. *Working Document 1/2009 of the Article 29 Working Party on 'Pre-trial Discovery for Cross Border Civil Litigation*,' WP 158, adopted by the Working Party on 11 February 2009, *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf [hereinafter WP 158].

perhaps with the introduction of further global agreements along the lines of the Hague Convention."[7]

The Working Document is of particular value because it describes the key factors which should guide litigants when considering the disclosure of documents for the purposes of litigation where EU data protection law may apply to the personal data contained in those documents.

The Working Document recognises that there is a balance of interests between those of the litigant and those of the individuals who are the subject of the personal data which may be disclosed in litigation. However, it does not consider in any detail the practical risks which may affect individuals as a result of the litigation process and how those risks could be mitigated.

RETENTION OF DATA—THE LEGAL HOLD

In common law systems it is the duty of litigants, as soon as litigation is reasonably anticipated, to preserve all documents which may be relevant to that litigation. This is a very old rule which has been elaborated in the light of the prevalence of information in electronic form, but without changing the fundamental duty to retain documents. In the United States, the retention of data in these circumstances is commonly known as a "legal hold."

EU data protection law requires data controllers to hold personal data no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[8] The Working Document recognises that a legal hold, even one imposed by a U.S. court, may make the continued storage of relevant data "necessary" for such purposes.[9]

---

7. *Id.* at 2.
8. Data Protection Directive, *supra* note 4, art. 6(e).
9. WP 158, *supra* note 6, at 8.

However, if a data controller is entitled to retain data for the purpose of a legal hold, can it continue to make use of that data? For example, can a business analyse its old data for marketing/segmenting purposes? Can it sell products or services, such as legal expenses insurance, to persons whose personal data is affected by a legal hold and with the knowledge that they are so affected? Can it use the data for the purposes of assessing someone's credit rating?

It is possible to see in such circumstances that the existence of a legal hold might almost benefit a company, in that it would have an excellent excuse to suspend its document destruction policy and make use of the information contained in the retained documents. Individuals, on the other hand, might be placed at a disadvantage.

It is clear that, under current EU data protection legislation, documents subject to a legal hold cannot be subject to unrestricted use. The other principles of the Data Protection Directive, such as the duty to process data fairly and lawfully and not to process data for purposes which are incompatible with the purposes for which the data was originally obtained,[10] would continue to apply.

In practice the mere retention of data should not adversely affect individuals. What is more important is how that data is used. Unfortunately, neither the Data Protection Directive nor the draft Regulation give guidance on the continued use of data when its retention period has been extended beyond what would otherwise have been expected. For example, is it automatically unfair to continue the processing of data for normal business purposes when, other than for the existence of a legal hold, that data would have been destroyed? If so, that would tend to suggest that the requirement that data be held no

10. Data Protection Directive, *supra* note 4, arts. 6(a)-(b).

longer than necessary is a superfluous one, as it is all part and parcel of the fairness principle. That would be a surprising conclusion.

Perhaps a better solution would be some more explicit guidance on the degree to which retention periods can be relaxed in the case of legal holds. It could be made clear that any additional processing should be limited to that required by the legal hold. In practice this would mean that data which would otherwise have been deleted, but which is retained as a result of a legal hold, should be removed from live access, and used only for the purposes of the litigation to which it relates.

IDENTIFYING RELEVANT DATA

The Working Document recognises that document reviews carried out for the purposes of litigation may satisfy the "legitimate interests" test in Article 7(f) of the Data Protection Directive (considered further below) and are therefore permissible. Where litigation is taking place outside the EU it recommends that, in order to ensure that the interests of the parties are properly balanced, the initial review exercise designed to determine which documents are relevant to the litigation should generally take place within the EU.[11] These exercises will typically involve an extensive analysis of the data available to the data controller who is subject to a duty to disclose documents in the litigation. To save time and money, the review may be aimed not just at identifying relevant documents, but also at identifying arguments which could be put forth in the litigation and narrowing key issues between the parties.

In the course of the review exercise, it is frequently the case that unrelated material comes to the attention of the person conducting the review. That person may in some circumstances

11. WP 158, *supra* note 6, at 11.

feel duty-bound to disclose that data to others, even though it has no relevance to the litigation.

For example, an email which appears during the review process may disclose that an employee may have been guilty of a criminal offence or, perhaps, some conduct which is not illegal but may be regarded as immoral or in breach of his or her employment contract. There may be extensive gossip conducted on email which is against company policy.

A strict interpretation of the law would lead to the conclusion that reviewers should process (i.e., filter and review) the data only for the purposes which had been identified as legitimate, namely the identification of relevant documents and the selection of evidence which could be used in support of the contentions of the litigating party. Use for other purposes would not be permissible. However, it is not realistic to expect that reviewers would ignore unrelated material which is potentially damaging to the custodian of the documents.

There is little or no guidance as to how reviewers should act in such a case. Given that the material might (apart from a legal hold) have been deleted, it is arguably appropriate that there should be a general rule that reviewers should consider the material made available to them only for the purposes of the litigation, and should not make any broader use or disclosure of that material save in very exceptional circumstances. Processing for the purposes of the prevention or detection of crime is arguably already included in the current law,[12] and needs no additional protection, but it seems right that reviewers should also be entitled to inform their principal if (say) employees have engaged in bullying, aggressive, or discriminatory conduct which

12. *See* Data Protection Directive, *supra* note 4, art. 13(1)(d) (which leaves the scope of the exception very much in the hands of Member States).

falls short of the criminal standard but is nevertheless contrary to company policy.

PRIVATE CORRESPONDENCE

The treatment of private correspondence is rather difficult. Many companies try to prohibit their employees from using corporate systems for the purpose of private correspondence, although the legality of such prohibitions is dubious in the light of the generally recognised right (under the European Convention on Human Rights) for individuals to conduct private correspondence.[13] The right to private correspondence may also be guaranteed in the constitutions of EU Member States.[14] Interceptions of private communications may be unlawful under national statutes.[15] Accordingly, the general guidance which one must give reviewers is that material which is apparently private should not be reviewed. Of course, private communications may be reviewed accidentally, because there may have been no indication that the communications were private and had no relevance to company business.

The trouble is that the special treatment given to private correspondence enables persons who are engaged in potentially illicit activity an avenue for communication which is arguably too easy. "Private" correspondence may not really be private at all. There is, accordingly, an argument that it should be permis-

---

13. Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8.1, November 4, 1950, 213 U.N.T.S. 221 ("Everyone has the right to respect for his private and family life, his home and his correspondence."); *see also* Halford v. United Kingdom, 24 Eur. Ct. H.R. 523 (1997).

14. *See, e.g.*, CONSTITUTION OF THE KINGDOM OF THE NETHERLANDS, art. 13; CONSTITUTION OF THE PORTUGUESE REPUBLIC, art. 34.

15. *See, e.g.*, Regulation of Investigatory Powers Act, 2000, 2000 c. 23, s. 1 (U.K.).

sible for an independent person to carry out a review of correspondence conducted using company systems, which purports to be private, in order to ensure that the correspondence in question is truly private and does not relate to the litigation. Such a person would need to be, clearly, above reproach and under the strictest obligations of confidentiality.

At present the law does not clearly allow this, but it is possible that the new Regulation may affect the position. The original draft of the Regulation issued in January 2012 stated (in Recital 15) that it did not apply "to processing of personal data by a natural person which are exclusively personal, family-related or domestic, such as correspondence." This might have continued the difficulty. However, the current draft[16] states (in Recital 15) that it does not apply "to processing of personal data by a natural person in the course of a personal or household activity, and thus without a connection with a professional or commercial activity. Personal and household activities include social networking and online activity undertaken within the context of such personal and household activities." It may be argued that this narrows the definition of what is truly "private" and may enable an independent person to establish in a particular case whether purportedly private correspondence really is "without a connection with a professional or commercial activity." However, the draft Regulation makes no clear reference to this. In the absence of a system which allows a data controller to be satisfied that correspondence is genuinely private without breaking the law, the likelihood is that, in practice, the law will be broken.

16. Document 9565/15, *supra* note 3, at 9 (Text approved by the Council of the European Union on 15 June 2015).

DISCLOSURE OF DATA

When data is disclosed from one jurisdiction to another—particularly when data is disclosed from the European Union to a destination in the United States—there is a clear risk that individuals may become subject to investigations or proceedings which they would not otherwise have suffered. For example, sanctions regimes in the U.S. and the European Union are different, and conduct which is entirely lawful within the European Union may be deemed to be unlawful in the United States. Nevertheless, U.S. authorities may seek information regarding EU persons who have engaged in conduct which it considers to be unlawful.

From the point of view of the individual, it may seem unjust that the disclosure of documents in litigation should expose that person to risks which that person would otherwise not have faced. This is a constant concern encountered in practice when considerations of disclosure arise. It requires, in turn, a very careful consideration of the legal basis for the disclosure of data from one entity to another.

The Working Document reviews the various possible legal bases for disclosure, but in practice the one which is most commonly used is where the disclosure is in the legitimate interests of the disclosing party, or the party to whom documents are to be disclosed, and those interests are not outweighed by the privacy interests of the relevant individuals.[17] This legal basis requires a balancing test between the rights of the parties and

17. Data Protection Directive, *supra* note 4, art. 7(f). For more detail on this test, *see Opinion 06/2014 of the Article 29 Working Party on the 'Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC,'* WP 217 (April 9, 2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (68 pages of discussion).

the individuals which "should take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject."[18]

Unfortunately there is little guidance as to how that test should be applied where disclosure would put the data subject at risk of additional legal proceedings. For example, if such a risk can be identified, is this of such significance that the interests of the parties to the litigation are completely overridden, and disclosure should not be made? A complicating factor is that the parties to the litigation may not have real control over the use of the documents when they leave the EU—a U.S. government agency, for example, may show an interest in documents which have been supplied for civil litigation, and may demand them irrespective of the wishes of the parties.

Another problem is that it is difficult to predict how documents may be used, and what their individual importance may be, unless the circumstances of the individual are well known to the disclosing party. It may be, for example, that a U.S. agency already has several pieces of a jigsaw which it is trying to put together and needs the documents to complete the picture, but the significance of those documents in achieving that result may be obscure to others.

There is no perfect solution to this conundrum. A pragmatic approach may be as follows. If it can be shown that an act of disclosure may put someone at risk of proceedings (whether criminal or civil) which they would not otherwise have faced, the burden should then be on the disclosing party to demonstrate that, despite this, disclosure is nevertheless fair. This will not be an easy burden to discharge. It might be possible to do so if it can be shown that there is no significant increase in the practical risk to the individual's property or liberty as a result of the

18. WP 158, *supra* note 6, at 10.

disclosure. But if there is such a risk, then in respect of that individual the case for disclosure is not made out. It should be noted that Article 7(f) of the Directive requires an analysis of "the interests for fundamental rights and freedoms of the data subject"—in other words, each data subject must be considered separately and not as members of a class.

RIGHTS OF DATA SUBJECTS

One of the rights of data subjects under the Data Protection Directive is to have access to the data held about them.[19] This right tends to be used more frequently where data controllers process large volumes of customer data (e.g., in the financial services industry) or in the case of employment disputes. It is unusual for it to be exercised where the data subject wishes to know what data concerning him or her is being used in litigation in circumstances where the data subject is not a party to the litigation itself, but data subjects in such circumstances have the same rights of access as others. Of course, in practice, data subjects may not be aware that their data is being used in litigation, even though they should be told—see below.

Data subjects also have the right to rectification, erasure, or blocking of data where it is not being processed in accordance with data protection law,[20] but this right is rarely exercised in any formal sense.

Unfortunately for data subjects, while they are entitled to know what data about them is being processed, it is not easy for them to find out what may happen to their data. The Directive states that, in response to an access request, they must be told of "the recipients or categories of recipients to whom the data are disclosed," but this does not in terms require data controllers to

19. Data Protection Directive, *supra* note 4, art. 12(a).

20. Data Protection Directive, *supra* note 4, art. 12(b).

tell data subjects every time their data are disclosed to someone else. The UK Data Protection Act puts it differently, stating that data subjects must be given "a description of . . . the recipients or classes of recipients to whom [the personal data] are or may be disclosed."[21] This is not likely to provide any helpful information to data subjects.

The Working Document reminds us of the transparency rules in Articles 10 and 11 of the Directive, saying that the information requirements in these Articles "would require advance, general notice of the possibility of personal data being processed for litigation. Where the personal data is actually processed for litigation purposes, notice should be given of the identity of any recipients, the purposes of the processing, the categories of data concerned and the existence of their rights."[22]

This is, arguably, a counsel of perfection. In practice, in the United Kingdom, which is the largest common law jurisdiction in the EU, notification procedures such as these are rarely observed in litigation, and their use in this field is not the subject of any detailed guidance from the UK Information Commissioner. They do not form part of the UK Civil Procedure Rules. Such notices would, in any event, have little meaning for data subjects and might well worry them unnecessarily.

In short, the notice provisions in the legislation are rather vague and inadequate. They do not ensure that data subjects will receive any useful information (indeed, in practice one must question whether exercising the right of subject access in any circumstance provides data subjects with information of real use in any but a tiny minority of cases). It would be much

21. Data Protection Act 1998 s. 7(1)(b), *available at* http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf.

22. WP 158, *supra* note 6, at 11.

better if data controllers were subject to clearer duties which informed them when it is appropriate to bring matters to the attention of data subjects. Thus, for example, it is clearly of interest to data subjects to know that personal data concerning them is of key importance in a case and may result in them being called as a witness. It is of less interest to them to know that their name (along with those of hundreds of others) has been included in a list of employees which has been disclosed in circumstances where their involvement in the case is likely to extend no further.

CONCLUSION

The theme throughout this brief paper is that more detailed, practical guidance is required for litigants in common law proceedings in order to enable them to comply with data protection law and to protect the interests of data subjects. The European Commission's aim that the new Regulation will give data subjects more control over their personal data will not be realised if there is uncertainty over the application of the law because of the lack of guidance. Whatever the final form of the new EU law, it is to be hoped that guidance can be developed, either through Opinions of the Article 29 Working Party or through national regulatory authorities.