Florida Journal of International Law

Volume 18 | Issue 3 Article 2

December 2006

Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas

Scott Rempell

PRIVACY, PERSONAL DATA AND SUBJECT ACCESS RIGHTS IN THE EUROPEAN DATA DIRECTIVE AND IMPLEMENTING UK STATUTE: *DURANT V. FINANCIAL SERVICES AUTHORITY* AS A PARADIGM OF DATA PROTECTION NUANCES AND EMERGING DILEMMAS

Scott Rempell[*]

I. INTRODUCTION 808

II. PRIVACY AND DATA PROTECTION 811
A. *The Difficulty in Defining Privacy* 811
B. *The Bases of Data Protection* 812

III. THE EMERGENCE OF DATA PROTECTION LAWS 813

IV. THE EU DATA DIRECTIVE AND DATA PROTECTION LAW IN THE UNITED KINGDOM 816
A. *The EU Data Directive* 816
B *Data Protection in the United Kingdom* 817

V. THE *DURANT* SAGA 819

VI. A FAULTY STATUTORY ANALYSIS 823
A. *"Relate to" Does Not Support the* Durant *Court's Narrow Construction of Personal Data* 823
B. *The Opinion and Intent Clauses Indicate a Wide Personal Data Definition* 825
C. *DPA Section 7 Does Not Connote a Data Subject Focus Requirement* 827

VII. PERSONAL DATA AND SUBJECT ACCESS RIGHTS 830
A. *Effective Data Protection Laws Necessitate an Overly Broad Personal Data Definition* 831

---

* J.D., American University Washington College of Law, *magna cum laude*, Order of the Coif, Editor-in-Chief of the *American University International Law Review*; B.A., University of Michigan, James B. Angell Scholar. Prior to attending law school, Scott Rempell served as an editor and writer at the Center for Social and Legal Research, a think tank founded by Dr. Alan Westin that focused on privacy issues and published *Privacy and American Business*. The author is currently an appellate litigator at the U.S. Department of Justice, Civil Division. The views expressed herein are only attributable to him. In memoriam Leon Posin.

B. *Obstacles in Formulating a Narrower Personal Data Definition* 834
C. *The Effects of Personal Data on Subject Access Rights* 837

VIII. CONCLUSION 840

I. INTRODUCTION

European data protection laws regulate information practices when the information qualifies as "personal data." Sweeping in nature, personal data under the European Data Directive (Directive) is any information relating to an identified person or a person identifiable through direct or indirect means.[1] Critics denounce this one size fits all regulatory approach, arguing, inter alia, that all "personal" data need not qualify for the panoply of data constraints imposed on information falling under the umbrella of data protection laws.[2] Equally consequential are the subject access rights afforded under data protection laws, which provide individuals with access to their personal data held by third parties.[3] Retrieving such information can be a daunting task for any entity collecting personal information; seldom will one find a public or private organization that does not collect personal data in one form or another. Cross-border information systems and complex organizational structures compound the difficulties, as well as increasing the time and cost of complying with subject access requests.[4]

The recent high-profile case of *Durant v. Financial Services Authority* is an ideal springboard for discussing personal data and subject access rights. Michael Durant complained to the Financial Services Authority (FSA), which regulates the UK banking industry, about possible fraudulent

1. Directive 95/46, art. 2(a), 1995 O.J. (L 281) 31, 38 (EC) [hereinafter Directive].

2. *See, e.g.*, Andrew Charlesworth, *Information Privacy Law in the European Union:* E Pluribus Unum *or* Ex Uno Plures?, 54 HASTINGS L.J. 931, 941-42 (2003) (relaying concerns expressed by industry associations, regulatory bodies and others). The European Privacy Officers Forum argues that the scope of the personal data definition should be guided by the level of potential harm that data may pose to an individual. *See* EUROPEAN PRIVACY OFFICERS FORUM, COMMENTS ON REVIEW OF THE EU DATA PROTECTION DIRECTIVE (DIRECTIVE 95/46/EC) 3-4 (2003), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/lawreport/paper/epof_en.pdf. Providing no such harm, professional data warrants exclusion from the definition of personal data. *Id.*

3. *See, e.g.*, Directive, *supra* note 1, at 42, art. 12; Data Protection Act, 1998, c. 29, § 7 (Eng.).

4. *See* Ulrich U. Wuermeling, *Harmonisation of European Union Privacy Law*, 14 J. MARSHALL J. COMPUTER & INFO. L. 411, 445 (1996).

activity at Barclays Bank (Barclays) when he was a customer there.[5] Durant asserted his right under the UK data protection statute to access all his personal data held by FSA.[6] Subsequently, FSA stated that the results of the investigation into Barclays were not Durant's personal data and the Court of Appeal agreed.[7] Since the information did not qualify as Durant's personal data, he was not entitled to access the information.[8]

The business community welcomed the court's holding,[9] the UK Information Commissioner quickly offered clarification,[10] and many commentators questioned its viability.[11] However, subsequent UK decisions affirmed the narrow interpretation of personal data emanating from the *Durant* case.[12] Undeterred, Durant complained to the House of Lords[13] and the European Commission (EC) formally voiced its concern that the United Kingdom was not complying with the Directive requirements.[14] In December 2005, Durant's pending appeal in the House of Lords ended without any further resolution.[15] Durant is now considering

---

5. Durant v. Financial Services Authority, [2003] EWCA (Civ) 1746, [10].

6. *Id.* [11].

7. *Id.* [11]-[17], [27].

8. *Id.* [27]-[28].

9. *See Guidance Welcomed on Subject Access but Fears* Durant *Flawed*, DATA PROTECTION L. & POL'Y, Feb. 2004, ¶ 5 (explaining that a pragmatic interpretation of the DPA is generally good news for the business community); *see also Bad Law Due for a Reform*, W. DAILY PRESS, Mar. 10, 2004, at 10 (claiming that the DPA is a "dismal" and complicated piece of legislation and the *Durant* court's decision will make life easier for companies who bear the burden of the data protection provisions without getting anything in return).

10. *See* INFORMATION COMMISSIONER'S OFFICE, THE '*DURANT*' CASE AND ITS IMPACT ON THE INTERPRETATION OF THE DATA PROTECTION ACT 1998, at 1-11 (2004).

11. *See UK's Data Protection Act Might Not Meet European Union Standards*, OUT-LAW, May 19, 2004, ¶¶ 5-6 [hereinafter *UK's Data Protection Act*], http://www.out-law.com/page-4549 (last visited Dec. 13, 2005) (relaying concerns that the court's decision does not stand up to scrutiny in areas concerning CCTV systems and name recording, and that the court exceeded the permissible level of judicial discretion under the Act).

12. *See* Johnson v. Medical Defence Union Ltd., [2004] EWHC (Ch. D) 347, [13] (contending that the *Durant* decision profoundly impacted interpretation of the DPA and restricted the rights of those making subject access requests).

13. Durant filed papers with the European Commission in Brussels in early May 2005. *UK's Data Protection Act*, *supra* note 11, ¶ 4.

14. *See European Commission Suggests UK's Data Protection Act Is Deficient*, OUT-LAW, July 15, 2004, paras. 1-3, http://www.out-law.com/page-4717 (last visited Dec. 13, 2005) (discussing how a European Commission spokesman confirmed sending a letter to the United Kingdom regarding potential noncompliance of several DPA provisions with the Directive requirements, and expressing the general belief that the letter focuses on the *Durant* court's interpretation of personal data).

15. *See Durant Ends His Data Protection Battle*, OUT-LAW, Dec. 10, 2005, http://www.out-law.com/page-6218.

action in the European Court of Human Rights and the UK Information Commissioner is scrambling to offer further guidance; the European Commission would not initiate infraction proceedings while *Durant* was pending in the courts, but now such proceedings are viable.[16]

This Article critiques the court's decision in *Durant* and uses the issues of the case to further analyze the appropriate parameters of personal data and subject access rights under data protection laws in Europe. Part II surmises the notions of privacy and data protection to help show the ambiguity in the rights being codified in data protection statutes. A brief synopsis of the emergence of data protection laws in Europe are presented in Part III, followed by an overview of the Directive and data protections laws in the United Kingdom in Part IV. With the necessary understanding of the technical terminology used in the Directive and DPA, Part V then discusses the *Durant* case.

Part VI offers a critique of the court's statutory interpretation, pointing out three specific instances where the court erroneously ignored drafters' intent. The statutory analysis will serve to highlight how the shortcomings are in the court's interpretation of UK data protection law; the law itself does not require reform. In Part VII, this Article will use the *Durant* rationale for limiting the definition of personal data to show that the current scope of personal data is necessarily "sweeping" and not subject to any narrowing interpretation. Next, Part VII highlights the variables needed to create a more limited personal data definition; the discussion shows the difficulty in eliminating certain categories of data from the personal data definition. With the necessarily broad personal data definition in mind, Part VII then argues for a reevaluation of the subject access provisions in European data protection laws.

This Article concludes by challenging those opposed to the current breadth of the personal data definition to develop a more limited definition

16. "The *Durant* case is extremely important to the [European] Commission. . . . It is of fundamental important because if the British interpretation of what is private data is upheld then it could seriously undermine the EU Directive." Joe Kirwin, *More Privacy Action Against UK, Germany Appears Likely, EU Diplomats Say*, BNA PRIVACY L. WATCH, Jan. 20, 2006 (recounting the sentiments of an anonymous EU official, who added that despite ongoing negotiations with the UK government, subsequent action is likely in the near future); *see also* Tom Blass, *Refused Appeal in UK Case Leaves Definition of 'Personal Data' Intact for Now*, BNA PRIVACY L. WATCH, Dec. 16, 2005; *Durant Ends His Data Protection Battle*, *supra* note 15 (relaying the UK government's contention that the European Commission's misinterpretation of *Durant* is responsible for the inquiry); *Post-*Durant *Narrow Definition of "Personal Data" Remains Intact*, DATA PROTECTION L. & POL'Y, Dec. 2005 ("Durant is now considering an appeal to the European Court of Human Rights under Article 6 (right to a fair trial) and Article 8 (the right to privacy)."); *UK IC Considers Advice Update as House of Lords Out of* Durant *Review*, DATA PROTECTION L. & POL'Y, Oct. 2005.

based on the issues and dilemmas discussed. An additional challenge is posed to those in favor of the current scope of personal data—to develop a limiting framework for subject access rights accounting for both the need to provide a high level of privacy protection and the ongoing and future problems in the current framework.

II. PRIVACY AND DATA PROTECTION

A. *The Difficulty in Defining Privacy*

Scholars and courts habitually disagree on a uniform definition of privacy that encompasses all attributes of the term.[17] Privacy definitions have focused on autonomy rights,[18] information control,[19] or control over intimate information.[20] Other attempts at codification define privacy through a set of interrelated attributes[21] or through a personhood perspective.[22] Divergent privacy explanations have fostered debate as to

17. *See* COLIN J. BENNETT, REGULATING PRIVACY 12-13 (1992) (explaining how privacy is a controversial term encompassing a "confusing knot of problems, tensions, right, and duties," and stating how the meaning of privacy is often dependent on the particular time and circumstances when scholars evaluate its parameters).

18. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890-1891) (advocating that privacy protections secure the "right to be let alone"); *see also* Les P. Carnegie, *Privacy and the Press: The Impact of Incorporating the European Convention on Human Rights in the United Kingdom*, 9 DUKE J. COMP. & INT'L L. 311, 323 (1998) (recounting the definition of privacy espoused by the UK Committee on Privacy and Related Matters in 1990, which stated that privacy amounts to protection against intrusions into an individual's personal life through direct means or publication of personal information).

19. ALAN WESTIN, PRIVACY AND FREEDOM 7 (1970) (contending that privacy derives from control over information from the collection stage through the information dissemination practices of individuals, groups, or institutions).

20. *See* LEE A. BYGRAVE, DATA PROTECTION LAW: APPROACHING ITS RATIONALE, LOGIC AND LIMITS 129 (2002) (relaying commentators' contentions that information dissemination does not amount to a loss of privacy rights if the information is not sensitive or intimate); *see also* Jonathan P. Graham, Note, *Privacy, Computers and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1407 (1987) (noting how backers of the intimacy-oriented privacy protection theory believe that information sensitivity levels derive from shared societal expectations, not individual subjective beliefs).

21. Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428-36 (1980) (proposing a privacy framework that encompasses secrecy, solitude and anonymity, and reviewing the interrelation between the three terms).

22. *See* BYGRAVE, *supra* note 20, at 129. EU Member States express concerns that individuals' difficulty determining the amount and type of personal information held by others negatively impacts personality development. *Id.*

whether privacy is a value in itself or merely a means of achieving other ends.[23]

The proffered justifications for protecting privacy include allowing individuals to define themselves and the information they want to share with others in the formation of relationships.[24] Proponents also argue that privacy provides for emotional release,[25] invites self-evaluation, facilitates decision-making,[26] and promotes physical and psychological autonomy.[27] Autonomy—like many of the other bases offered in support of privacy protection—is potentially a defining attribute, end purpose, or a means to other purposes.[28] The semantic obscurity intrinsic in this causal chain exemplifies the difficulty in conceptualizing and defining privacy.[29]

B. *The Bases of Data Protection*

Data protection is easier to define than privacy because it focuses on informational rights.[30] Alan Westin's well-known information privacy definition allows for control over the timing, purpose, and extent of communications that contain personal information.[31] The scope of citizens' actual control over personal information under data protection laws is not so inclusive, but the definition exemplifies a number of fair information principles central to data protection laws: transparency; rectification; data quality; collection, use and disclosure limitation; data security; and rights enforcement.[32]

---

23. Such scholars focus instead on a functional analysis, based on the effects of gaining or losing privacy. Graham, *supra* note 20, at 1408.

24. *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 484 (1968).

25. Emotional release from "continuous physical and psychological confrontations." WESTIN, *supra* note 19, at 37-38.

26. *See id.* at 37 (reasoning that much creative thought derives from evaluative processes most often utilized in moments of solitude).

27. *See* Graham, *supra* note 20, at 1397.

28. *See* BENNETT, *supra* note 17, at 33 (comparing differing interpretations).

29. Poignantly stated by Oscar Ruebhausen, privacy is "part philosophy, some semantics and much pure passion." Oscar M. Ruebhausen, *Foreword* to WESTIN, *supra* note 19, at x.

30. Data protection is a more precise term because it distinguishes both the policy considerations inherent in discussions of privacy values and privacy's philosophical dimensions. BENNETT, *supra* note 17, at 13-14.

31. WESTIN, *supra* note 19, at 7 (stating how such control fosters an individual's temporary withdrawal from social participation through various means).

32. *Cf.* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 45-47 (1997) (examining how European countries' data protection principles generally adhere to four overarching themes: requiring certain responsibilities for personal information; ensuring that processing of personal data occurs in an open and transparent manner; creating special protections for sensitive data; and ensuring effective enforcement methods and oversight of personal data processing practices).

Although data protection is easier to define than privacy, setting forth the appropriate purposes for data protection triggers an equally broad discussion as seen with the given purposes for protecting privacy. Many European data protection initiatives have a human rights grounding,[33] which include the right to privacy and other recognized fundamental freedoms such as protection of liberty, the right to self-determination, and freedom of thought.[34] Additionally, proponents argue that individual autonomy and other attributes furthered by data protection are essential to foster pluralistic,[35] democratic societies.[36] Data protection initiatives may also find their grounding in economic concerns.[37]

III. THE EMERGENCE OF DATA PROTECTION LAWS

Shortly after World War II, the Council of Europe (Council) made privacy a distinct right.[38] Legislatures erected legal regimes establishing

---

33. *See* BYGRAVE, *supra* note 20, at 108-09 (explaining how experiences with fascism in the years leading up to and during World War II played a particularly important role in creating fears over privacy threats).

34. *See id.* at 38, nn.114-16, 125 (reviewing current and repealed data protection statutes listing objectives beyond the protection of privacy, such as protecting human identity and personal integrity); *cf.* Personal Data Act, 2000, No. 31, § 1 (Nor.) (stating the objectives of the data protection laws of Norway, which is not a member of the European Union, including protection of private life and the protection of personal integrity).

35. *See* BYGRAVE, *supra* note 20, at 135 (conveying how privacy safeguards secure pluralism by ensuring the continuance of diversity in expressed ideas and lifestyle choices).

36. *See* BENNETT, *supra* note 17, at 32 (explaining how informational privacy fosters a specific kind of democracy, which includes the traits of individualism and a market-driven economy); *see also* Ruth Gavison, *To Early for a Requiem: Warren and Brandeis Were Right on Privacy vs. Freedom of Speech*, 43 S.C. L. REV. 437, 461-62 (1992) (arguing that privacy fosters human dignity, autonomy and self-direction, and these attributes encourage active participation in decision-making at a community level). Public and private organizations' information dossiers can manipulate individuals' behaviors and desires, and such abuse is a threat to liberty and democracy. PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 6 (1998). Even when such information is held by private organizations, governments often access private sector information. *Id. Contra* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 731 (1987) (relaying the point of view that publicity, not secrecy, is the key to ensuring a healthy democratic decision-making process).

37. *See* BYGRAVE, *supra* note 20, at 112-13 (arguing that economic and other technology-drive benefits will not fully materialize if citizens do not have faith that companies are adhering to fair information practices). Potential data embargoes provide another incentive for setting data protection standards. *Id.*

38. *See* Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Europ. T.S. No. 5 (Nov. 4, 1950) [hereinafter Human Rights Convention] (affirming a right to

protection for citizens' private affairs in the aftermath of the war as a means of denying public officials the degree of scrutiny previously afforded to Nazi party leadership.

Technological progression made the collection, use, and dissemination of personal information easier and cheaper.[39] International organizations responded by directly confronting privacy threats from technology in the late 1960s.[40] European nations followed in the next few years, passing data protection statutes and making citizens' right to privacy more tangible.[41] As a result, the otherwise elusive concept of privacy began to take the form of specific informational privacy rights; those handling personal information now had enumerated responsibilities in situations implicating individuals' right to privacy.

As the right to privacy became more robust among European legal regimes, divergent data protection laws threatened Member State integration efforts.[42] Data protection efforts culminated when the Council passed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council Convention) in 1981, with the objective of facilitating integration by setting guiding privacy principles.[43] The United Kingdom passed its first comprehensive data

---

privacy in one's personal affairs and prohibiting unjustifiable interference into individuals' private and family life by public authorities); *see also* CATE, *supra* note 32, at 43-44 (recounting how European privacy laws are deeply rooted in a desire to avoid the situation in World War II, where Gestapo and Nazi regimes sought to control the population); EUR. PARL. ASS. DEB. (4-464) 145 (June 14, 1995) (remarking on the importance of assuring high confidentiality standards to "avoid the threat of the shadow of Big Brother in Europe"); *cf.* Universal Declaration of Human Rights, G.A. Res. 217A, at 73-74, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc. A/810 (Dec. 12, 1948).

39. *See* Graham, *supra* note 20, at 1395 (noting how computers play a part in numerous aspects of a person's life and reviewing the types of information becoming progressively easier to exchange, including heath data, purchase information, and details on familial relations). Organizations take full advantage of these technological advances in their data practices. *Id.*

40. International efforts to address privacy concerns started with the 1967 meeting of the International Commission of Jurists, which represented one of the first international efforts to discuss the right to privacy as a fundamental right. BENNETT, *supra* note 17, at 131-33 (1992); *see also* Human Rights and Scientific and Technological Developments, G.A. Res. 2450, at 54, U.N. GAOR, 23d Sess. (1968) (suggesting the need to address threats to privacy rights from technological and scientific advances by conducting future studies to determine a course of action for achieving the appropriate balance between technological progress and competing interests).

41. *See* CATE, *supra* note 32, at 32 (noting that the national push for data protection standards began when the German state of Hesse enacted data protection legislation in 1970, and continued with Sweden's subsequent 1973 data protection statute).

42. *See* Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, pmbl., Europ. T.S. No. 108 (Jan. 28, 1981) [hereinafter Council Convention].

43. *Id.* arts. 2-12; *cf.* Org. for Econ. Cooperation & Dev., *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum,*

protection law in 1984 (1984 DPA),[44] largely in response to fears that the United Kingdom's trading partners might block data from entering its borders.[45]

Continued efforts to foster greater economic and political unity in Europe[46] led to a more detailed draft data protection proposal in 1990.[47] After five years of negotiations and amendments,[48] the European Union passed the Directive[49] to protect privacy and other fundamental freedoms, and harmonize Member State data protection laws.[50] The United Kingdom abstained from voting on the Directive,[51] but obliged with its implementation requirements and passed the Data Protection Act (DPA) in 1998.[52]

Introduction, O.E.C.D. Doc. C(80)58/Final (Sept. 23, 1980), *reprinted in* 20 I.L.M. 422, 427. The Council Convention places a greater emphasis on the need to protect privacy than the OECD Guidelines. CATE, *supra* note 32, at 34.

44. Data Protection Act, 1984, c. 35 (Eng.) (repealed 1998); *see also* Ronald Wellington Brown, *Economic and Trade Related Aspects of Transborder Data Flow: Elements of a Code for Transnational Commerce*, 6 NW. J. INT'L L. & BUS. 1, 24 (1984) (noting that civil libertarian groups did not think the 1984 DPA was broad enough in scope to adequately protect privacy); BENNETT, *supra* note 17, at 93 (reviewing the twenty-three year gap between the government's initial privacy legislative proposal and the actual enactment of a data protection bill, and noting how commentators gave the 1984 DPA mixed reviews).

45. *See* BYGRAVE, *supra* note 20, at 113. Computer manufacturers expressed concern that the industry would suffer without a data protection law; the UK government gave these industry voices significant credence. BENNETT, *supra* note 17, at 90-91.

46. *See* CATE, *supra* note 32, at 35.

47. Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1990 O.J. (C 277) 3.

48. *See, e.g.*, Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1992 O.J. (C 311) 30 [hereinafter Amended Directive Proposal].

49. Directive, *supra* note 1; *see* SWIRE & LITAN, *supra* note 36, at 25 (conveying how the Directive's goal of creating a uniform data protection standard is a logical outgrowth of the European desire to create a "unified internal market" among its Member States). *See generally* Treaty Establishing the European Economic Community, art. 249, Mar. 25, 1957, 298 U.N.T.S. 36 (discussing how Directives define objectives that Member States must adopt through any legislative mechanism they deem appropriate).

50. *See* Directive, *supra* note 1, at 38, art. 1 (stating that a person's right to privacy is a fundamental right, but forbidding Member States from using the right to privacy as an excuse to restrict data flows between Member States).

51. The Council approved the Directive on Oct. 24, 1995 because adoption only required a majority vote. EDWARD WOOD, THE DATA PROTECTION BILL [HL]: BILL 158 OF 1997-98, at 11 (Res. Paper 98/48, 1998).

52. Data Protection Act, 1998, c. 29 (Eng.).

IV. THE EU DATA DIRECTIVE AND DATA PROTECTION LAW IN THE UNITED KINGDOM

In contrast to the abstract rights-based reasons for creating data protection statutes, the actual terminology used in data protection laws is quite technical and intricate. European and Member State data protection laws rely extensively on a group of triggering definitions to define the contours of information protection. The next two sections will provide an overview of the central terms used in *Durant*.

A. *The EU Data Directive*

The Directive provides extensive protection for information on natural persons[53] through broad-based definitions. Information must constitute personal data in order to activate many of the Directive's provisions.[54] As previously noted, data becomes personal when it relates to an identified person or a person identifiable through direct or indirect means.[55] Identifiable means include a person's specific "physical, physiological, mental, economic, cultural or social" attributes.[56]

Personal data also directly or indirectly triggers most of the remaining Directive definitions. When information relates to an identified or identifiable natural person, that person becomes the "data subject."[57] "Processing" involves any operation performed on personal data through any means.[58] Any natural or legal person responsible for personal data processing becomes a data "controller,"[59] and those carrying out the processing are "processors."[60] Structured and accessible personal data constitute a "filing system."[61]

Some consider the subject access rights contemplated under Article 12 as the most important fair information principle.[62] The data subject is

53. "Legal" persons do not qualify for protection. Directive, *supra* note 1, at 38-39, art. 2.

54. *Id.* at 39, art. 3; *cf.* Durant v. Financial Services Authority, [2003] EWCA (Civ) 1746, [21] (explaining that the issues of the case are moot if the data in question does not satisfy the threshold requirement of constituting personal data).

55. *See* Directive, *supra* note 1, at 38, art. 2(a).

56. *Id.*

57. *Id.* at 38, art. 2(a).

58. *Id.* at 38, art. 2(b). Processing includes collecting data, using data, and transferring data to third parties.

59. *Id.* at 38, art. 2(d).

60. *Id.* at 38, art. 2(e).

61. *Id.* at 38, art. 2(c).

62. *See* CATE, *supra* note 32, at 103.

entitled to any data held by a data controller "relating to"[63] the individual requesting the data.[64] The Directive's subject access rights give the data subject the unconstrained ability to confirm if data controllers are processing the requester's information and to inquire into the purposes for such processing, as well as the right to request communication of the processed data in an intelligible form.[65] Data subjects are also entitled to information on the logic behind automated data processing, at least for certain classes of data "concerning"[66] the data subject.[67]

B. *Data Protection in the United Kingdom*

Data protection was formally codified in the United Kingdom twenty-one years ago when the government passed the Data Protection Act 1984. The Directive's requirements go beyond the 1984 DPA's data protections. The 1984 DPA enumerated the core fair information principles, but since the personal data and processing definitions trigger many of the data protection principles, the DPA drafters believed that these 1984 DPA definitions were too narrow.[68] Under the 1984 DPA, personal data is data relating to an identifiable living individual.[69] The definition includes expressions of opinion about an individual, but specifically excludes indications of data controller intentions regarding the data subject, such as the intent to take part in a future business decision based on the data subject's information.[70] "Processing" personal data under the 1984 DPA occurs when a data user performs a list of enumerated operations on the

---

63. *See infra* text accompanying notes 92-93 (observing the meaning and scope of the words "relate to" in the UK data protection law's definition of personal data).

64. Directive, *supra* note 1, at 42, art. 12 (stating that a data controller must provide confirmation of personal data processing "relating to" the data subject, and providing additional requirements when the data subject receives affirmative confirmation); *see also id.* at 35, rctl. 41 (reciting how the Directive provides access rights to enable a person to ensure data accuracy and lawfulness of processing).

65. *Id.* at 42, art. 12.

66. *See infra* text accompanying notes 108-20 (reviewing the distinction between "relate to" and "concerning" in the Directive subject access provisions).

67. Directive, *supra* note 1, at 42, art. 12 (providing data subjects with the additional right to rectify, block, or erase personal data that is not in accordance with the Directive, as well as the right to notification about third party data sharing when such notification is possible and does not require a "disproportionate effort").

68. *See* Lords Hansard, Feb. 2, 1998, col. 476 (noting that DPA compliance requires an expansion of the processing definition); House of Lords, Official Report of the Grand Committee on the Data Protection Bill, Feb. 23, 1998, cols. CWH5-H6.

69. Data Protection Act, 1984, c. 35, § 1(3) (repealed 1998).

70. *Id.*

data, but only when such performance is done "in reference to the data subject."[71]

In response to the sense among UK data experts that these definitions were too narrow, the United Kingdom passed the DPA in 1998 to bring its national law in line with the Directive requirements.[72] "Processing" information or data occurs by obtaining, recording, holding, or performing any operation on such information or data.[73] A "relevant filing system" refers to information relating to an individual that is not processed by automatically operated equipment, but that is structured in a manner that fosters accessibility to information relating to a particular individual.[74]

The DPA's personal data definition departs from the wording of the Directive and 1984 DPA personal data definitions.[75] Under the DPA:

> "Personal Data" means data which relate to a living individual who can be identified-
>
> (a) from those data, or
>
> (b) from 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.[76]

"Data subject" is defined separately as "an individual who is the subject of personal data."[77] A person determining the purposes and manner of current or future personal data processing is a "data controller."[78] A "data processor" is anyone processing data on behalf of a data controller, unless that person is an employee of the data controller.[79]

---

71. *Id.* § 1(7).

72. *See* Lords Hansard, Feb. 2, 1998, cols. 472-75.

73. Data Protection Act, 1998, c. 29, § 1(1) (explaining that operations include alteration, retrieval, use, disclosure, or dissemination of information or data); *see also id.* § 1(2) (listing the default rule for the scope of obtaining, recording, using, and disclosing, as they relate to personal data, which include performing those operations on information contained in the data).

74. *Id.* § 1(1) (conveying how information is structured in a readily accessible way when it refers to an individual or by reference to specific criteria relating to an individual).

75. *Compare supra* text accompanying notes 55-56 (reviewing a Directive personal data definition based on identifiability), *with* text accompanying *infra* note 76 (defining a DPA personal data definition specifically connoting future data collection likelihood, and more specifically addressing certain types of matters, such as data controller intentions).

76. Data Protection Act, 1998, § 1(1).

77. *Id.*

78. *Id.*

79. *Id.*

The DPA separately reviews data subjects' right to access their personal data held by a data controller in Part II of the Act. Section 7 requires that data controllers inform individuals when controllers process "personal data of which that individual is the data subject."[80] If data controllers process such personal data, the data subject has a right to obtain the personal data in an intelligible form.[81] Furthermore, data subjects have a right to information on the logic behind automated processing decisions when such decisions significantly affect the data subject.[82] The broadened scope of the personal data definition under the DPA creates a greater chance that data held by third parties activates subject access rights and the other Directive requirements implemented under the DPA.

V. THE *DURANT* SAGA

Durant v. Financial Services Authority involves two primary parties, Michael Durant and FSA. Durant was a customer of Barclays and the FSA regulates the UK financial services sector. Barclays sued Durant for failing to pay a mortgage loan and the court ruled for the bank in 1993.[83] Durant's subsequent charge of fraud against the bank was unsuccessful.[84] Durant sought to reopen his complaint against the bank and around July 2000, he sought assistance from FSA.[85] In March 2001, FSA concluded its investigation in Barclays, but refused to provide investigatory details to

---

80. *Id.* § 7(1)(a) (explaining that the data controller obligation extends to processing done on behalf of the data controller, and that the obligation is triggered by a subject access request); *see also* Data Protection Act, 1984, c. 35, § 21(1) (repealed 1998) (imposing a similar obligation to inform an individual of personal data retention when the requestor is the data subject and utilizes the law's afforded access rights).

81. Data Protection Act, 1998, c. 29, § 7(1)(c) (adding that the data subject also has a right to obtain information on the sources of the data in the data controller's possession).

82. *Id.* § 7(d) (indicating that the automated decision must be the sole basis for the decision, and the data controller must also use the personal data for evaluating matters such as data subject creditworthiness and performance at work); *see also* House of Commons, Standing Committee D, Data Protection Bill, May 12, 1998 [hereinafter Commons Standing Committee] (reviewing an amendment to the subject access provisions to clarify the meaning of "automated" in light of a common association between the term and "computerized data").

83. Durant v. Financial Services Authority, [2003] EWCA (Civ) 1746, [10]. Mr. Durant was the guarantor of a £120,000 loan; the court did not accept his defense that Barclays never advanced the money. Durant v. Financial Services Authority, [2003] EWCA (Civ) 573, [2].

84. *Durant*, EWCA (Civ) 573, [2].

85. *Durant*, EWCA (Civ) 1746, [10] (remarking how Mr. Durant believed that the FSA's supervisory role over Barclays may yield documentation beneficial to his case against the bank).

Durant[86] because of confidentiality requirements set forth under applicable UK banking law.[87]

Durant made two subject access requests under Section 7 of the DPA, demanding disclosure of all his personal information in the possession of FSA.[88] FSA refused to disclose information held in its manual files, arguing that the information was not Durant's personal data.[89] Durant initiated court action, but both district and county court judges ruled against him.[90] The Court of Appeal, Civil Division, granted Durant permission to appeal.

The Court of Appeal approached the case by considering whether the information constituted personal data within the scope of the DPA. Durant argued for a broad personal data definition that encompasses all documentation creating an identifiable connection between the individual and his or her information.[91] FSA emphasized the importance of the words "relate to" in the definition of personal data, and argued that the narrower definition[92] of "have reference to, concern" was preferable over the

---

86. *Id.* (observing that in November 2000, the FSA Complaints Commissioner dismissed Mr. Durant's complaint concerning FSA's refusal to disclose the investigation records); *see also Durant*, EWCA (Civ) 573, [2] (noting how Barclays' later dismissal for misconduct of the bank manager who handled Mr. Durant's account increased Mr. Durant's suspicions of wrongdoing, and speculating on a causal relationship between the dismissal and the FSA investigation).

87. *Durant*, EWCA (Civ) 1746, [10] (relaying that Sections 82 to 85 of the Banking Act 1987 created the confidentiality requirements). The Financial Services and Market Act 2000 superceded and repealed the Banking Act 1987. Financial Services and Markets Act (consequential Amendments and Repeals) Order 2001, S.I. 2001/3649, § 3.

88. *Durant*, EWCA (Civ) 1746, [11]. *But cf. Details on File*, POST MAG., Apr. 15, 2004, at 40 (arguing that the purpose of the subject access provision is to enable persons to ensure data accuracy, not for the purpose of protecting or providing documents).

89. FSA also argued that the manual files were not subject to disclosure even if they did constitute personal data because the information was not part of a "relevant filing system" under Section 1(1) of the DPA. *Durant*, EWCA (Civ) 1746, [11].

90. *Durant*, EWCA (Civ) 573, [4]-[8]; *see also* Data Protection Act, 1998, c. 29, § 7(9) (authorizing court action by individuals who believe that a data controller has not properly complied with the subject access requirements under the Act).

91. *Durant*, EWCA (Civ) 1746, [24] (arguing that the documentation generated by Mr. Durant's complaint constitutes his personal data because he is the source of the data).

92. *Compare* Commons Standing Committee, *supra* note 82 (reviewing the dictionary definition of "logic" to aid in the discussion of Section 7(1)(d) of the DPA), *and* Ian McLeod, *Literal and Purposive Techniques of Legislative Interpretation: Some European Community and English Common Law Perspectives*, 29 BROOK. J. INT'L L. 1109, 1113-14 (2004) (admitting that the assistance of a dictionary is a useful tool, but stressing the importance of context), *with* Edward W. Cleary, *Evidence as a Problem in Communicating*, 5 VAND. L. REV. 277, 288 (1952) (averring that words are merely symbolic references connoting specified personal meaning, and that dictionary definitions provide "equivalent verbalizations; they send us on long tours of other words").

broadly encompassing definition of "have some connection with, be connected to."[93] FSA also contended that the personal data definition's inclusion of expressions of opinion (opinion clause) and controller intentions toward the data subject (intent clause) indicates that data does not "relate to" an individual in the absence of these qualifications.[94]

The Court of Appeal ruled in favor of FSA, approving its narrower interpretation of personal data and finding that the information sought by Mr. Durant did not constitute his personal data.[95] The court reasoned that data only becomes personal when it affects a person's privacy.[96] Data's effect on a person's privacy is a function of its location on a continuum of relevance or proximity to the data subject, whereby "effects" increase as the link between the data and the data subject becomes closer.[97]

The court set forth two criteria central to determining the nature of data on the privacy continuum. The first notion is whether or not the data is significantly biographical; that is, where the data conveys information beyond a person's mere involvement in a particular occurrence.[98] The second measurement involves the data focus, where data becomes less personal as the person moves from being the focus of the data to a tertiary player that merely has some level of involvement with the actual object of the data compilation.[99]

---

93. *Durant*, EWCA (Civ) 1746, [25].

94. *Id.* (concluding that the inclusion of such expressions, as well as similar distinguishing sub-sections in the subject access provisions, would become unnecessary if "relate to" is given a broad definition).

95. *Id.* [31] (finding that while Mr. Durant initiated the complaint, the objects of the information sought concerned Barclays and FSA).

96. *Id.* [28] (arguing that data's affect on a person's privacy is not dependent on the aspect of a person's privacy affected, so personal and familial information, as well as information about a person in his or her business capacity, may all qualify as personal privacy affecters). *But cf.* SIMON CHALTON, REFLECTIONS ON *DURANT V. FSA*, http://www.twobirds.com/english/publications/articles/Reflections_on_Durant_v_FSA.cfm (last visited Dec. 13, 2005) (claiming that the Directive's protections are not limited to individuals' right to privacy).

97. *Durant*, EWCA (Civ) 1746, [28] (proposing that a document's mere mention of a data subject's name does not necessarily affect the data subject's privacy and confer the subject access rights afforded by the DPA for personal data).

98. *Id.*

99. *Id.* (asserting that a person's instigation into the conduct of another is an example of a scenario where the instigator's level of involvement does not make that person the focus of the data). The court used a case recently decided in the European courts to support the proposition that data is not personal unless it affects a person's privacy. *Id.*; *see also* Case C-101/01, Lindqvist v. Kammaraklagaren, 2203 E.C.R. I-12971, 1 C.M.L.R. 20, ¶¶ 24, 27 (2004) (finding that the posting of an individual's name, in conjunction with a telephone number, working conditions, or other attributes on the internet, constitutes processing by automatic means because the combination of

The court began with the proposition that the DPA purports to faithfully reproduce the Directive's intent to allow individuals to obtain access to their personal data.[100] The purpose of the subject access provisions in the Council Convention, Directive, and DPA, according to the court, is to permit a data subject to obtain information that a data controller may use to unlawfully infringe a data subject's privacy.[101] Furthermore, since Section 7(1)(b)(i) of the DPA permits access to personal data when an individual is the "data subject," the court opined that the DPA requires that an individual is the focus of the data.[102] The court also agreed with FSA's contention that the opinion and intent clauses would lack meaning if the court broadened the scope of personal data, since the clauses specifically enumerate certain types of data considered personal.[103] Since the DPA did not entitle Mr. Durant to the documentation, the court concluded that Mr. Durant's subject access request was a "misguided" attempt to utilize the DPA to obtain third party discovery.[104]

---

a name and another personal attribute "undoubtedly" satisfies the threshold Directive requirement that the data be personal).

100. *Durant*, EWCA (Civ) 1746, [26].

101. *Id.* [27].

102. *Id.* [29].

103. *Id.*

104. *Id.* [31] (pointing out that litigants should not be able to expand the definition of personal data in an attempt to use the DPA as a tool to obtain discovery when the information sought would not satisfy discovery relevancy requirement). The court went on to rule on the relevant filing system issue, holding that the files in question were not part of a relevant filing system, which requires the data controller to discern the existence of information capable of constituting personal data at the beginning of the search, and that information must also be part of a filing system sufficiently sophisticated to indicate the location of such personal data. *See id.* [45]-[51] (observing the similarity between the DPA and the Directive, and stating that the Directive supports the narrow interpretation of a relevant filing system); *see also* INFORMATION COMMISSIONER'S OFFICE, *supra* note 10, at 1 (relaying the Information Commissioner opinion that the court's personal data and relevant filing system rulings were the most important aspects of the decision). The court concluded by finding that the DPA does not provide Mr. Durant the right to obtain the redacted information and that the court has wide discretion under Section 7(9) of the DPA, even though the provision is not relevant in the present case. *See Durant*, EWCA (Civ) 1746, [60]-[67] (striking a balance between the rights of third parties to protect documentation containing their personal data with the rights of the individual making the access request); *see also id.* [74] (agreeing with previous case law that interpreted court discretionary authority as "general and untrammelled").

VI. A FAULTY STATUTORY ANALYSIS

The Court of Appeal interpretation of the DPA is inconsistent with the Directive. As explored in Part VII of this Article, the Directive's all-encompassing definition of personal data is not subject to any limiting interpretation. It is necessary to analyze the specific interpretation set forth by the Court of Appeal because of the potential action regarding UK compliance with the Directive in the European courts,[105] and the UK government's current insistence that fault lies in the misconstruction of the *Durant* opinion, rather than an erroneous rationale itself.[106] There are two possible reasons why the court's holding could be considered incorrect: either (1) the DPA's personal data definition is flawed, or (2) the court's interpretation of the definition is incorrect. Should the UK interpretation of personal data be found erroneous, the former reason would require the United Kingdom to redraft the personal data definition. In the absence of action in the European courts, understanding the underlying reasoning of the *Durant* opinion is still vital; the case has created striking confusion about compliance obligations in the United Kingdom.[107] This Article argues that, in fact, the DPA personal data definition is consistent with the Directive requirements. The three sections that follow demonstrate how the erroneous holding is the result of an incorrect analysis by the Court of Appeal.

A. *"Relate to" Does Not Support the* Durant *Court's Narrow Construction of Personal Data*

The Financial Services Authority correctly asserted that "relate to" has multiple meanings, but the court improperly used a narrower version of "relate to" to limit the scope of personal data in the DPA. The court's holding affirms FSA's contention that the words "relate to" in the DPA personal data definition means "have reference to, concern" instead of "have some connection with, be connected to." The court did not specifically consider the statutory construction of the term, but found that personal data requires focus, and FSA contended that "have reference to, concern" requires a "more or less direct connection."[108]

The statutory construction of the Directive and DPA subject access provisions show that "relate to" connotes a broad interpretation of personal data. Article 12(a) of the Directive entitles a data subject to confirmation

105. *See supra* note 16 and accompanying text.
106. *See supra* note 16 and accompanying text.
107. *See infra* text accompanying notes 194-95.
108. *Durant*, EWCA (Civ) 1746, [25], [28].

of data processing "relating to him."[109] The data subject is only entitled to communication of the logic behind automated processing decisions for data "concerning him" for the matters enumerated in Article 15(1).[110] Under Article 15(1), the logic communication requirements apply to a limited class of data, including creditworthiness, work performance, and other matters concerning or significantly affecting the data subject.[111] The Directive drafters would have no reason to use distinct terms in the subject access provisions if "relate to" is synonymous with "concern."[112] In fact, the Directive drafters amended an earlier version of Article 12(a), which stated that a data subject is entitled to information on processing purposes "about" the data subject.[113] The current version permits access to information for the purpose of data processing "relating to" the data subject,[114] reflecting a conscious decision to amend the wording.[115] Therefore, "concern" clearly connotes a more limited class of data triggering the logic communication requirements.[116]

---

109. Directive, *supra* note 1, at 42, art. 12 (requiring data controllers who confirm such processing to provide the data subject with information on the purpose for processing the data).

110. *Id.* (stating that the automated decisions listed in Article 15(1) provide a floor of situations where data processors must provide data subjects with information about processing logic); *see also id.* at 35, rctl. 41 (reciting the subject access distinction between general subject access rights for information relating to the data subject and data subject's right to know the logic behind certain automated decisions concerning the data subject).

111. *Id.* at 43, art. 15 (noting that in addition to legal effects concerning the data subject or decisions significantly affecting the data subject, a data subject's right to decline a specific decision also requires that the decision is solely based on automated personal data processing).

112. *See generally* FRANCIS BENNION, STATUTORY INTERPRETATION: A CODE § 141, at 350 (2002) (reviewing the technique of precision drafting, where drafters aim to use language accurately and consistently).

113. *See* Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1992 O.J. (C 94) 173, 185 [hereinafter 1992 Directive Amendments].

114. Directive, *supra* note 1, at 42, art. 12(a) (permitting access to information on processing purposes after the data controller confirms processing information relating to the data subject).

115. *See generally* BENNION, *supra* note 112, § 80, at 243 (explaining that when a statute does not expressly amend a previous statute, the newer Act is impliedly amended if necessary to avoid inconsistency). By implication, where legislators do amend the legislation in question, the latter wording is controlling. *See id.* (stating how two inconsistent texts are not concurrently valid).

116. *Cf.* Philip Coppel, *Environmental Information: The New Regime*, 2005 J. PLAN. & ENVTL. L. 12, 16 (noting that the definition of "environmental information" in Environmental Information Regulation 2004 is limited to information "on" one of the enumerated categories, while the previous 1992 environmental regulation definition encompasses information that "relates to" the environment). The author concludes that "on" restricts the scope of the former "relates to" definition. *Id.*; *see also* Council Directive 2003/4, art. 2, 2003 O.J. (L 41) 26, 28 (stating the environmental information definition, which includes the word "on," that Environmental Information Regulation 2004 faithfully reproduces).

DPA Sections 7(1)(a) and (b) transpose the Directive's Article 12(a) conditions by requiring data controller information disseminated to a requesting individual who is the data subject of personal data processing.[117] Section 7(1)(d) codifies an equally limited data class requiring logic communication.[118] Even though Section 7(1)(d) does not specifically include the word "concerning," it limits the logic requirement to situations involving significant effects on the data subject.[119] The omission is simply a shorthand form of the Directive requirement. DPA Section 7(1)(d) codifies Article 15(1) of the Directive; Article 15(1) states the minimum scope of the Article 12(a) logic requirements. These DPA subject access provisions parallel the Directive requirements.[120] Thus, the Directive makes a clear distinction between "relate to" and "concerning," giving "relate to" a broader meaning than "concerning." Therefore, "relate to" in the DPA personal data definition does not narrow its applicable scope; the court incorrectly applied the narrower version of "relate to" in order to justify factors like focus.

B. *The Opinion and Intent Clauses Indicate a Wide Personal Data Definition*

The court incorrectly held that the opinion and intent clauses narrow the personal data definition because the DPA drafters inserted the clauses to emphasize that both types of information constitute personal data. The DPA's inclusion of the clauses is subject to two interpretations. Under the first interpretation—which is consistent with the court's opinion—a broadly defined classification is limited to the particular subclasses

117. Data Protection Act, 1998, c. 29, § 7(1)(a)-(b) (noting that the requirement applies even when others are processing personal data on behalf of the data controller, and requiring a description of the personal data, the purposes for the processing, and a list of the data recipients when personal data processing occurs).

118. *Compare id.* § 7(1)(d) (relaying the components of automated processing, data controller evaluations, and decisions significantly affecting the data subject), *with* Directive, *supra* note 1, at 43, art. 15(1) (listing the components of automated processing, data controller evaluations, and decisions with significant effects or legal effects on the data subject).

119. Data Protection Act, 1998, § 7(1)(d) (discussing how data controllers must relay logic information for certain evaluative decisions when the automated personal data is either solely or likely the sole basis for decisions significantly affecting the data subject).

120. Parliament rejecting an amendment to the subject access provisions due to concerns that the amendment would upset the link between the logic requirements and automated processing decisions. Commons Standing Committee, *supra* note 82. This is the causal chain taken straight from the Directive. *See* Directive, *supra* note 1, at 42-43, arts. 12-15.

subsequently and inclusively listed in the definition.[121] A contrary interpretation is that the legislators merely sought to highlight how the general definition of personal data encompasses both expressions of opinion and intentions of data controllers and others.[122]

The legislative history of the DPA[123] and its juxtaposition with the 1984 DPA demonstrate that the latter interpretation is correct. The 1984 DPA definition of personal data included expressions of opinion, but specifically excluded intentions of data controllers.[124] The House of Lords' Grand Committee on the Data Protection Bill added the intentions clause to solidify that personal data includes data controller intentions and eliminate confusion to the contrary.[125] Accordingly, the court's holding does not account for the legislative purpose behind the opinion and intent clauses. The holding is an incorrect statutory interpretation and improperly makes the DPA inconsistent with the Directive.

Beyond the drafters' intent lies a more straightforward reason why the opinion and intent clauses do not narrow the personal data definition. Factual data warranting DPA protection does not require an opinion, and

---

121. *See* BENNION, *supra* note 112, § 390, at 1072, § 393, at 1076 (summarizing the *expressio unius* principle, which means that "to express one thing is to exclude another" and explaining that if "A includes B," the words of extension imply that A includes subclasses other than B, and that those additional subclasses do not fall under the statutory definition in question).

122. *See id.* § 395, at 1078 (contending that the *expressio unius* principle does not apply when there is an apparent alternative reason for singling out specific terms or phrases). It is a common drafting device to include certain matters as inclusive within a definition for the purpose of avoiding future arguments as to whether the matters in question are within the definition's scope. *Id.* § 378, at 1050-51.

123. There is a general prohibition against the use of Parliament proceedings during the passage of a bill under the exclusionary rule. *See id.* § 220, at 545; *see also* McLeod, *supra* note 92, at 1109-11 (reviewing the changing dynamics of the English legal system by starting with the premise that English courts are rooted in a common law tradition built on the legislative interpretation process of literalism). However, UK case law has relaxed this general prohibition to permit the use of parliamentary materials to resolve ambiguities and prevent literal interpretations that would lead to absurd conclusions when the materials clearly reveal legislative intentions regarding ambiguities and obscurities, and where the materials involve statements from a bill's promoters. *See* Pepper v. Hart, [1993] 1 All E.R. 42, 69 (H.L.); *see also* Pickstone v. Freemans PLC, [1988] 2 All E.R. 803 (H.L.) (remarking how UK bills incorporating European legislation under the European Communities Act of 1972 represent a "special category" warranting exception to the exclusionary rule).

124. Data Protection Act, 1984, c. 35, § 1(3) (Eng.) (repealed 1998).

125. House of Lords, *supra* note 68, cols. CWH6-H7 (asserting that the government originally believed that data controller and others' intentions fell within the personal data definition, but that the amendment would put any potential ambiguities to rest).

the intent clause only involves data triggered by third party actions.[126] Accordingly, the court's narrowing interpretation excludes data relating to an identifiable person merely because the data is neutral without inclusion of opinions or third party intentions.[127] Such an interpretation even excludes data that is both biographical and focused on the data subject—the two factors used by the court to gauge the definition of personal data.

To illustrate this point, consider an individual who visits a health professional and fills out a medical form containing factual health information, where the form contains no additional information provided by a data controller or other data processor. Despite the absence of opinions or third party intentions, the health form reveals biographical information focused on the data subject, and contains information on medical symptoms and other data. Such information is not only personal data, but sensitive personal data.[128]

The court's desire to curtail one specific subject access request led to an inappropriate limiting rationale that excludes highly intimate information under the opinion and intent clause analysis. The court's reasoning contradicts clear legislative intent and disregards the need to protect various categories of data—including sensitive information if the court's opinion and intent clause analysis is taken at face value. It is clear that the opinion and intent clauses do not support a narrow personal data definition, and the court improperly used the clauses to support such a conclusion.

C. *DPA Section 7 Does Not Connote a Data Subject Focus Requirement*

Durant misconstrued the wording of the DPA subject access provisions and incorrectly used the provisions as proof of a narrow personal data definition. The court found that the DPA's personal data application to the subject access provisions narrowed the scope of personal data because the DPA entitles an individual to access personal data "of which . . . [he] is the

126. *See* Data Protection Act, 1998, c. 29, § 1(1) (listing the opinion clause and intent clause before stating "of the data controller or any other person in respect of the individual").

127. *See* Durant v. Financial Services Authority, [2003] EWCA (Civ) 1746, [80] (Buxton, L.J., concurring) (claiming that FSA's investigation would trigger the DPA if it expressed an opinion about Mr. Durant, but not if the FSA opinion were solely directed at Mr. Durant's complaint).

128. *See* Data Protection Act, 1998, § 2(e) (labeling physical and mental health information, or data on a specific health-related condition, as sensitive personal data); *see also* Directive, *supra* note 1, at 40-41, art. 8 (providing heightened protection for special data categories and labeling health data as one of those special categories).

data subject."[129] Without previously discussing the definition, the court inferred that this phrase has a narrowing effect by connoting focus.[130] This interpretation is incorrect because an individual does not qualify as a data subject until after that individual's information qualifies as "personal." Additionally, the court's interpretation would have the effect of making the current scope of "processing" meaningless.

Durant improperly applied the subject access provision's reference to a "data subject" to narrow the personal data definition because "data subject" is a circular term that provides no additional support for the court's conclusion.[131] The Directive does not separately define a data subject. It parenthetically notes in the personal data definition that information relating to an identified or identifiable person is synonymous with the term data subject.[132] An individual thus becomes a data subject when the data satisfies the definition of personal data. The DPA separately defines a data subject, but the definition is equally dependent on the information qualifying as personal data.[133] Since personal data is a necessary condition to trigger the term "data subject," the court cannot rely on a data subject reference to narrow the scope of personal data.

The court also failed to consider that its holding on the meaning of "data subject" would nullify changes made to the DPA "processing" definition. The 1984 DPA drafters limited the processing definition to operations performed "by reference to the data subject."[134] In 1991, the UK Data Protection Tribunal (now the Information Tribunal)[135] interpreted this clause to limit processing to operations focused on the data subject.[136] Both

---

129. *Durant*, EWCA (Civ) 1746, [29] (asserting that the use of the term "data subject" in the subject access provisions picks up its interpretory meaning through its application in the DPA personal data definition).

130. *See generally id.* [22], [29] (mentioning the notion of a "data subject" in the Council Convention and Directive without elaborating on its meaning before discussing its effect on the definition of personal data).

131. *See* BENNION, *supra* note 112, § 199, at 485 (explaining how circularity is a common drafting error, and a typical example of statutory circularity is when a definition uses the defining term in the explanatory part of the definition).

132. Directive, *supra* note 1, at 38, art. 2(a).

133. Data Protection Act, 1998, § 1(1) (defining a data subject as "an individual who is the subject of personal data").

134. Data Protection Act, 1984, c. 35, § 1(7) (Eng.) (repealed 1998).

135. *See generally* Information Commissioner's Office, Tribunal Decisions, http://www.informationtribunal.gov.uk/ (last visited Dec. 13, 2005) (providing an overview on the appeals procedure after the Information Commissioner issues a notice, which may be issued for breaching the DPA).

136. *See* Equifax Europe Ltd. v. Data Protection Registrar, Data Protection Tribunal, Appeal Decision, ¶ 49 (1991), *available at* http://www.informationtribunal.gov.uk/Files/ourDecisions/

Houses of Parliament rejected amendments to add "by reference to the data subject" to the DPA processing definition.[137] The House of Commons Standing Committee proffered that such a limitation was contrary to the Directive's requirement of much wider personal data and processing definitions.[138] Accordingly, the 1984 DPA definition would not comply with the Directive if Parliament passed the amendment.[139]

Section 7(1) does not contain the phrase "by reference to the data subject" and the drafters knew the significance of this phrase for focus purposes.[140] The proper interpretation of "data subject" does nothing to save the court's disregard for the changes to the DPA "processing" definition. The subject access provisions do not support a personal data definition limited by focus or otherwise narrowed[141] and the court

---

equifax.pdf (indicating that Parliament intended the processing definition to focus on the data subject, and disputing the contention that the phrase requires an interpretation from the vantage point of a computer operator).

137. Commons Standing Committee, *supra* note 82 (suggesting the amendment in order to clarify that processing is limited to information relating to an identifiable person).

138. *Id.*

139. *Id.*

140. *See, e.g.*, Lords Hansard, Feb. 2, 1998, col. 446 (expressing concern that the processing definition without the phrase "by reference to the data subject" would catch personal data processing that does not directly concern the individual in question); *id.* col. 475 (responding that the Directive does not permit such a narrow construction).

141. *Cf.* Sue Cullen, *Subject Access: After* Durant*: Weaknesses in Judgment Highlighted*, DATA PROTECTION L. & POL'Y, May 4, 2004, ¶ 16 (arguing that the court incorrectly used the subject access sections to limit the scope of personal data because access rights concern matters beyond requester's personal data, such as the requirement that data subjects are entitled to information about data controller processing sources and logic). The validity of the author's contention is in part based on whether Section 7(1)(a) is a trigger to the other 7(1) subsections. *See* Data Protection Act, 1998, § 7(1) (listing the other subsections, which include data subjects entitlement to a description of their personal data, the purpose for the processing, communication of the personal data in an intelligible form and, in certain circumstances, the right to the data controller's logic for decision-making involving the data subject's personal data). Section 7(1)(b) starts by stating: "if that is the case," which refers to the Section 7(1)(a) requirement that data controllers inform data subjects if they are processing personal data. Consequently, Section 7(1)(b) is certainly dependent on Section 7(1)(a), but it is unclear if the beginning of Section 7(1)(b) modifies Sections (c) and (d). *See* BENNION, *supra* note 112, § 153, at 385-86 (defining general grammatical ambiguity as a universal doubt that exists independent of any particular factual scenario and providing an example where the issue is whether a phrase "govern[s] both limbs" or only one). Since Sections 7(1)(c) and (d) involve data subject rights regarding their personal data, it is likely that "if that is the case" in Section 7(1)(b) modifies all the subsequent section 7(1) subsections, since the contrary interpretation would grant hollow data subject rights. *See id.* § 155, at 387 (noting that considering opposing grammatical construction can aid in resolving grammatical ambiguities).

incorrectly interpreted the subject access provisions to support its incorrect, narrow construction of the DPA personal data definition.

VII. PERSONAL DATA AND SUBJECT ACCESS RIGHTS

The Court of Appeal held that data only warrants protection when "privacy" infringement is at play. While the Directive clearly mandates data protection for fundamental freedoms besides privacy,[142] thinking of these rights as inherently distinct is an unnecessary exercise in tautology. Other reasons given for protection go to some of the core bases scholars have used to justify privacy protection. Human identity, for example, may be considered one of the interrelated attributes used to define privacy.[143] Looking at the actual or potential effects of data processing on data subjects is therefore more valuable than trying to define privacy and subsequently working backwards to deduce data warranting protection.[144] With this notion in mind, the importance of context becomes clear when assessing data. Section A will explore the court's incorrect use of biographical information and focus data to show that contextual considerations mandate an all-encompassing definition of personal data. Section B explores the notion of personal data from a different vantage point, highlighting the factors that would have to be accounted for if the definition of personal data is to be successfully narrowed. Accepting the necessity of the wide definition and the infeasibility in successfully narrowing the definition of personal data, Section C will review how personal data's large scope intersects with the Directive's subject access provisions.

---

142. Directive, *supra* note 1, at 31, rctls. 1-3 (stating that data processing systems must respect privacy and other fundamental rights and freedoms, contribute to economic and social progress, and enhance individuals' well-being); *id.* rctl. 10 (proclaiming that the object of national data protection laws is protecting privacy and other fundamental rights and freedoms); Econ. & Soc. Comm., Opinion on the Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, 1991 O.J. (C 159) 38, 40 (recounting the Committee opinion that the Directive is not limited to privacy rights protection); 1992 Directive Amendments, *supra* note 113, at 175 (listing human identity as a distinct, protected right).

143. *See supra* note 21 and accompanying text. Human identity may also be thought of as an end, where personality development is the means, and scholars have argued that personality development is one of the central reasons for protecting privacy. *See supra* text accompanying note 22.

144. *See supra* text accompanying note 23.

A. *Effective Data Protection Laws Necessitate an Overly Broad Personal Data Definition*

The court's use of focus and biographical information as markers of privacy effecters to limit the definition of personal data highlights the importance of considering context in any privacy analysis. Data may affect individuals even if they are not the focus of biographical information directly stemming from a data entry.[145] In *Durant*, a data entry merely containing Durant's name yielded several inferences,[146] such as his financial affiliations and an association between Durant and fraudulent activity at a bank. A data entry saying "Mr. Durant has some relationship to fraudulent activity at Barclays" contains biographical information focused on Durant and would even qualify as personal data under the court's definition. Context can lead to inferences that include the same conclusion as the data entry, as well as other truthful and false inferences focused on Durant.[147] Focusing on the actual content of a particular data entry improperly negates the importance of contextual inferences; such inferences are potentially responsible for a particular negative end effect on an individual or a group collectively.

One need not look far to find an example illustrating the importance of contextual relevance. In *Johnson v. Medical Defense Union*, a case decided in the United Kingdom shortly after *Durant*, the Medical Defense Union (MDU) cancelled Johnson's membership, in part because he made too many service requests.[148] Johnson believed that the data entries were his personal data because the cancellation led others to infer that MDU

145. *See* BYGRAVE, *supra* note 20, at 131; *see also* Steven Lorber, *Data Protection and Subject Access Requests*, 33 INDUS. L.J. 179, 183 (2004) (highlighting that under the court's interpretation of personal data, CCTV, webcam recordings, and other unfocussed data potentially affecting privacy may not receive legal protection).

146. *See* DEPARTMENT FOR CONSTITUTIONAL AFFAIRS, HANDLING SUBJECT ACCESS REQUESTS UNDER SECTION 7 OF THE DATA PROTECTION ACT 1998, GUIDANCE PAPER, ¶ 7 (2002), *available at* http://www.dca.gov.uk/foi/dpasaguide.htm (indicating that name references are not always personal data, but the context of the listed name likely yields inferences qualifying the information as personal data).

147. *See, e.g.*, Johnson v. Medical Defence Union Ltd., [2004] EWHC (Ch. D) 347, [6], [8] (recounting that Mr. Johnson was distraught when a medical association did not renew his membership because expulsion leads to the inference that he is incompetent or committed some other wrong act that justified dismissal from the association); *cf.* BYGRAVE, *supra* note 20, at 46 (providing a rationale for a personal data definition that includes false opinions, at least when such opinions adversely affect the data subject). Bygrave contends that a false opinion adversely affects the data subject when the opinion is socially significant. *Id.*

148. *Johnson*, EWHC 347, [45].

ended his membership due to some sort of offensive behavior,[149] yet each individual entry merely stated Johnson's name and a brief time entry.[150] The fact that such entries resulted in MDU's membership non-renewal could lead to the inference that Johnson's dismissal was the result of some impropriety on his part;[151] the catalyst of the end effect—seemingly innocuous data entries—cannot be gauged in a vacuum.

Combined innocuous data creating a negative effect warrants protection. In the absence of an all-encompassing definition of personal data—as seen in the Directive and disregarded in *Durant*—the *Durant* court must theoretically create a guiding framework accounting for situations where seemingly innocuous data produces adverse consequences.[152] The court makes no such attempt, failing to consider that the perceived triviality of any data entry or inference is not dispositive because "privacy" effects are not entirely subject to objective measurements.[153] Particular data, and the inferences they yield or could potentially yield, impact individuals differently.[154] Specific individual reactions to seemingly mundane information may not even seem logical to a majority of people.[155] There are an unlimited amount of data types,

149. *Id.* [6].

150. *Id.* [44] (noting that each entry contained a very brief description of the advice sought, such as "Amorous patient").

151. *See id.* [6] (recounting how Mr. Johnson was "extremely concerned" about such a possibility based on what he described as his perceived "expulsion" from MDU).

152. As noted by Cate, "the privacy interests at stake in any given situation may vary from the profound to the trivial, and that valuation will depend significantly on who is making it." CATE, *supra* note 32, at 31; *cf.* Hrobjartur Jonatansson, *Iceland's Health Sector Database: A Significant Head Start in the Search for the Biological Grail or an Irreversible Error?*, 26 AM. J.L. & MED. 31, 50 (2000) (reasoning that the indirect identifiability determinations require consideration of the specific facts in a case based on a subjective interpretation); Graham, *supra* note 20, at 1430 (analyzing when data deserves legal protection and concluding that the data entries in question deserve consideration for their qualitative attributes, rather than the quantitative amount of factual information communicated).

153. *See* Econ. & Soc. Comm., *supra* note 142, at 40 (indicating that privacy practices may produce adverse consequences even if there is no tangible basis because perceived data controller privacy practices can foster public mistrust from ignorant or misinformed perceptions).

154. David Mallon has noted how seemingly trivial information on an employee's whereabouts may have significant effects if the employee's location becomes an issue of contention with his or her spouse. David Mallon, *Subject Access: Data Protection Act 1998: A Question of Perspective*, DATA PROTECTION L. & POL'Y, July 2004, ¶ 19.

155. *See, e.g.*, Charlesworth, *supra* note 2, at 941-42 (recounting organizations' concern that the personal data definition should not encompass professional data because such data presents no obvious privacy threat).

combinations, and processing techniques and purposes.[156] There is no uniform definition of privacy or formula for gauging subsequent infringement,[157] much less a more limited personal data definition that both encompasses all relevant information[158] and eliminates every data combination clearly lacking an adverse impact.[159]

Identifiability in the personal data definition, and its application to actual data practices, derives from a reasonableness standard based on particular processing situations.[160] The ambiguity in application of such a reasonableness standard is understandably frustrating to data processors, courts, and regulators.[161] However, any attempt to set rigid parameters on a personal data definition, as seen in *Durant*, is simply not feasible. The feasibility of such a narrowing interpretation presupposes the existence of

---

156. On organizations' pronouncements of their specific data processing practices, see, for example, Barclays, Privacy Policy: Personal Information, http://www.barclays.com/privacy/per_info.html (last visited Dec. 13, 2005); Lloyds TSB Bank PLC, Privacy, http://www.lloydstsb.com/privacy.asp?link=top_navigation (last visited Dec. 6, 2005).

157. *See supra* text accompanying notes 17-37 (reviewing competing privacy conceptions, as well as the different rationales and markers used to determine infringement).

158. Rule 401 of the Federal Rules of Evidence presents an interesting comparison to the difficulty in formulating a more limited personal data definition. Relevancy is not an inherent quality of any particular piece of evidence. Rather, relevancy derives from the relationship between an evidentiary item and a matter provable in a case. An item's relevance to a case may also be conditioned on the existence of an additional fact or facts. Presupposing the importance of a particular piece of data when formulating a personal data definition is equally suspect to hailing an evidentiary item's relevance before hearing the facts of the case. See FED. R. EVID. 401 advisory committee's note, for a further analysis of relevancy.

159. *See* DOUWE KORFF, THE FEASIBILITY OF A SEAMLESS SYSTEM OF DATA PROTECTION RULES FOR THE EUROPEAN UNION 12-14 (1998) (commenting that Member States do not even agree on the appropriate way to gauge the reasonableness standard of the Directive's broad personal data definition).

160. *See id.*; BYGRAVE, *supra* note 20, at 43 (stating how identifiability determinations are based on broad and flexible criteria); HOME OFFICE, DATA PROTECTION: THE GOVERNMENT'S PROPOSAL ch. 2, ¶ 2.3 (1997) (observing that the mere existence of other pieces of data does not create personal data, but such information is personal data if there is "a reasonable likelihood of the two pieces of information being capable of being brought together"). The expression "reasonable likelihood" is used in the Directive. *See* Directive, *supra* note 1, rctl. 26. This expression must presuppose that a data controller is aware of all present—and even future—data processing practices; an assumption whose validity seems ever declining as the complexity and size of an organization's information system increases.

161. *See* SWIRE & LITAN, *supra* note 36, at 47 (concluding that clear legal rules for data protection standards are essential for organizations investing in complex and expensive information systems that need to account for their processing obligations under data protection laws throughout Europe); *see also* Jonatansson, *supra* note 152, at 49-50 (noting that the Directive guidance on reasonability is not clear and does not provide enough information to effectively gauge the particular means necessary in making personal data determinations).

a readily discernable definition of privacy, and it is not surprising that the *Durant* opinion fails to define when information practices affect privacy. That certain data processing would not produce an adverse impact on a data subject is inapposite. Rather, the controlling issue is that no distinguishable category of information will both 1) *never* produce an adverse impact and 2) lend itself to discernable codification in law.

B. *Obstacles in Formulating a Narrower Personal Data Definition*

As previously noted, scholars have struggled to create a definition of privacy that encompasses all attributes of the term.[162] Distinctive expressions of opinion indicate a term denoting different things to different people. In the context of data protection, data somehow associated with an individual leads to some end effect on that person after data is processed. The distinction scholars draw is how exactly to describe the end effect, or, alternatively, how to label the culmination of values breached that caused the end effect. If the issue is control, as many suggest, then an individual's mere knowledge that another has his or her personal information might cause a negative psychological impact; or an affront on one's dignity.[163] Any of the proffered justifications for protecting privacy could produce a similar result; a negative psychological impact could derive regardless of the description used to explain privacy, be it a breach of perceived autonomy or the inhibition of self-reflection and decision-making.

Quite distinct from these effects against psychological well-being and one's dignity are tangible effects, such as a financial loss, as seen in the case of identity theft.[164] Identity theft also produces the loss of something else tangible, namely time, as it can take hundreds of hours to rectify. Moreover, the notion of loss of control over one's identity would produce

---

162. *See supra* text accompanying notes 17-29.

163. WESTIN, *supra* note 19, at 7; *see also supra* text accompanying note 22. While somewhat axiomatic, psychological well-being and dignity are not parallel. The term "psychological impact," is purposefully broad. The loss of dignity would lead to some end effect (some psychological impact). Dignity and the loss of psychological well-being are often linked; the premise for data protection in this discussion of "intangible effects" stems from many of the same justifications used by scholars to advocate privacy protection based on dignitary principles. *See generally* Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J. L. & TECH. 345 (1995).

164. Knowledge of individualized data used for authentication, notably in the financial services sector, can be particularly powerful. U.S. citizens' Social Security numbers present a prime example of data with a high potential to produce tangible effects.

a negative psychological impact, as would any "tangible" repercussion stemming from the misuse of one's personal data.[165]

If one were to try to measure the importance of protecting particular data, then consideration must be given to the probability of functional creep. Technological progression[166] and changes in sanctioned data processing[167] increasingly put data to uses beyond the initial intent of the party collecting the data. Functional creep also occurs when the collection of a particular data sample once limited to a narrow class expands to include a greater subset of people.[168] Equally apposite is unanticipated data

165. *See, e.g.*, Bell v. Mich. Council 25, No. 246684, 2005 Mich. App. LEXIS 353, at *22-23 (Mich. App. Feb. 15, 2005) ("Each [identity theft victim in this case] spent numerous hours trying to correct the problems created by the identity theft, which left their collective credit in ruins. Plaintiffs produced concrete examples of the aggravation and anguish suffered by detailing their experiences of trying to purchase cars, homes, furniture or phone service and the resultant humiliation of being turned down for credit.").

166. Notable examples are in the areas of biometrics and Radio Frequency Identification (RFID) technology. RFID technology identifies, marks and stores information electronically. "A radio frequency reader scans the tag for data and sends the information to a database, which stores the data contained in the tag." U.S. GOV'T ACCOUNTABILITY OFFICE, PUB. NO. GA0-05-551, INFORMATION SECURITY: RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT 4 (2005), *available at* http://www.gao.gov/new.items/d05551.pdf. For information on RFID technology and functional creep specifically, see *id.* at 20-22. Biometric identifiers include facial recognition, iris scans and fingerprints. For a concise overview of biometrics and the increasing use of biometrics in EU Member States for security purposes, see Electronic Privacy Information Center, Biometrics, http://www.epic.org/privacy/biometrics/.

167. Examples include increased sharing of data by law enforcement officials and increased collection of privately-held data by public agencies after 9/11. *See, e.g.*, Joe Kirwin, *EU Data Protection Office Says Retention Rules Need to Boost Individual Safeguards*, BNA PRIVACY L. WATCH, Dec. 27, 2005, http://news.com.com/europe+passes+tough+new+data+retention+laws/2100-7350_3-5995089.html (reviewing new requirements that telecommunications providers retain email and telephone data); Jo Best, *Europe Passes Tough New Data Retention Laws*, CNET, Dec. 14, 2005 (noting how advocates of the requirements praise the new legislation, which will "help trace terrorists through communications records").

168. The most obvious example is the collection of DNA samples, where the original justification for collection was in part premised on the limited class of dangerous felons forced to submit a sample. The catch in this type of process is that privacy activists are often pinned against a rationale with a highly pragmatic argument; in this case, the rationale is protecting the public against criminals. Thus, the privacy activist is pitted against concrete examples of suffering and misfortune, armed only with a quiver of abstract arrows. *See generally* Julia Preston, *U.S. Set to Begin a Vast Expansion of DNA Sampling*, N.Y. TIMES, Feb. 5, 2007, at A1 (discussing the role of immigration as well).

exposure. Data leaks, through intentional[169] or accidental means,[170] are an *inevitable* side effect of data processing.[171] If the justification for processing personal data—or the level of protection to be afforded personal data—is to be measured against some legitimate societal interest, then data leaks must be given a numerical measurement greater than zero.

Ideally, therefore, data protection would be determined by numerically evaluating data's 1) psychological/dignitary effect;[172] 2) tangible effect;[173] 3) likelihood of function creep;[174] and 4) likelihood of unanticipated data exposure.[175] The analysis is based on the data itself, in conjunction with data processor practices, standard operating procedures within a particular industry, and processor information systems. If the value outweighs the legitimate interest in collection, use or dissemination, then protection is warranted. Creating such a framework would theoretically point to data

---

169. Such as external security breaches and internal misuses by employees and others with 'legitimate' access to personal data. *See, e.g.*, Bob Sullivan, *California Employee Data Leaked*, MSNBC, May 28, 2002; *Group Claims "Thousands" of AOL Customer Credit Cards Stolen*, PRIVACY TIMES, June 27, 2000.

170. Accidentally posting sensitive information to an unsecured area of a website or bulk emailing mishaps are common mistakes. *See, e.g.*, Brian McWilliams, *Data Firm Exposes Records Online*, WIRED NEWS, Jan. 22, 2002, http://wired.com/news/privacy/0,1848,49893,00.html; Ariana Eunjung Cha, *Retirement Plan's Error Discloses Personal Data*, WASH. POST, Jan. 24, 2001, at E1; Pamela Whitby, *Cellphone Users' Confidential Data is Leaked on the Web*, BUS. DAY, Sept. 7, 1999.

171. Any dispute as to the prevalence and likelihood of data losses has been eliminated by the almost daily media accounts of data breaches and mishaps in the United States. *See, e.g.*, Tim Sandler, *New York Pulls Personal Data from Web*, MSNBC, Feb. 5, 2007; Greg Keizer, *VA Loses Another Hard Drive, Vet Data at Risk*, INFO. WK., Feb. 5, 2007; Joris Evers, *T.J. Maxx Hack Exposes Consumer Data*, CNET, Jan. 18, 2007.

172. For more information on the psychological/dignitary effect, see James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151 (2004); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1259-65 (1998).

173. For more on tangible effects, see, for example, Federal Trade Commission, ID Theft, http://www.consumer.gov/idtheft/; and Identity Theft Resource Center, http://www.idtheftcenter.org/index.shtml.

174. For a discussion on the concept of functional creep, see K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2 (2003); R. Brian Black, Note, *Legislating U.S. Data Privacy in the Context of National Identification Numbers: Models from South Africa and the United Kingdom*, 34 CORNELL INT'L L.J. 397, 408-09 & n.51 (2001); and Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1134 (2002) (limiting use of fingerprints taken for specific purpose); *see also* Kyllo v. United States, 533 U.S. 27 (2001). In *Kyllo*, the dissent criticizes Justice Scalia, writing the opinion of the Court, for basing the Court's holding on the implications of *future* uses for technology. *Id.* at 42-43 (Stevens, J., dissenting).

175. On data breaches, see Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 886-90 (2002).

processing warranting loosened protection. However, the analysis necessary to formulate each of these variables would be extraordinarily complex. Valuations of each variable present an additional problem, and the status of privacy as a fundamental right in Europe would make the threshold for protection especially low. The infeasibility in creating a viable framework highlights the rationale for the broad, all-encompassing definition of personal data under the Directive. The broad definition eliminates the "privacy effects" guess work, with limited exceptions such as the heightened protection for sensitive information afforded in the Directive.[176]

C. *The Effects of Personal Data on Subject Access Rights*

The catalyst of the *Durant* case was largely the juxtaposition of the personal data definition with the right to access one's personal data held by a data controller. The two are inexorably linked: the wider the definition of personal data, the greater the amount of information obtainable through a subject access request. As noted in the preceding section, the wide definition of personal data is certainly necessary. However, the potential ramifications of the interrelationship between these two provisions is kept at bay by a low amount of requests for access to personal data.[177] It is not surprising that the amount of requests is low, considering the infancy of the current data protection framework in Europe. Reports clearly show that citizens are largely unaware of their rights.[178]

The compliance costs of the access provisions to data controllers could be exorbitant[179] and difficulties tracking down vast amounts of intricately stored data can be very time-consuming.[180] However, the Directive does not mitigate data controller obligations based on the nature of subject access requests. Requesting assistance from a data subject, while

176. *See* Directive, *supra* note 1, at 40-41, art. 8.

177. EOS GALLUP EUROPE, DATA PROTECTION IN THE EUROPEAN UNION 46 (Flash Eurobarometer 147, 2003); *see also* COMMISSION OF THE EUROPEAN COMMUNITIES, FIRST REPORT ON THE IMPLEMENTATION OF THE DATA PROTECTION DIRECTIVE (95/46/EC) 9 (2003), *available at* http://europa.eu.int/ eur-lex/en/com/rpt/2003/com2003_0265en01.pdf.

178. EUROPEAN OPINION RESEARCH GROUP, DATA PROTECTION 49-50 (Special Eurobarometer 196, 2003) (indicating that less than a third of polled European citizens have heard about their subject access rights and noting that the average amount of citizens across Europe utilizing this right is seven percent).

179. *See* CATE, *supra* note 32, at 42 n.64.

180. *See, e.g.*, Lorber, *supra* note 145, at 180 (noting how such difficulties are "particularly acute" in the employment context).

permissible under the current Directive framework,[181] does little to rectify the compliance difficulties;[182] requesting assistance presupposes a data subject who is aware of how information is processed, or how particular processing situations can negatively impact them.

Compounding data subject awareness difficulties is data controller awareness of processing nuances. In the United Kingdom, for example, data controllers are instructed to weigh certain subject access considerations "against the effect on the data subject;"[183] words that ring hollow without any understanding of "effects." Is it based on the data controller's perception of how the data will affect the data subject? Or, conversely, is it based on the importance of the data as expressed by the data subject? Will the data controller weigh such effects differently if they are balanced against a perceived "inappropriate" use of the subject access provisions?[184] If so, "inappropriate" under what standards?

Several countries, including the United Kingdom, have requested changes to the Directive's subject access provisions.[185] The European Commission, however, has argued against amendments to the Directive. Commenting in a report gauging the implementation status of the Directive, the Commission noted:

> Experience with the implementation of the Directive is so far very limited. Only few Member States implemented the Directive on time. Most Member States only notified implementing measures to the Commission in the years 2000 and 2001, and Ireland has still not notified its recent implementation. Important implementation legislation is still pending in some Member States. This constitutes an inadequate basis of experience for a proposal for a revised Directive.[186]

---

181. COMMISSION OF THE EUROPEAN COMMUNITIES, *supra* note 177, at 15.

182. *See, e.g.*, Data Protection Regulations, 2000, S.I. 2000/191, *as amended by* S.I. No. 3223, *available at* http://www.opsi.gov.uk/Si/Si2000/20000191.htm (setting a maximum fee of £10 and limiting response time to forty days maximum).

183. INFORMATION COMMISSIONER, DATA PROTECTION ACT 1998, LEGAL GUIDANCE 46, *available at* http://www.ico.gov.uk/upload/documents/ library/data_protection/detailed_specialist_ guides/data_protection_act_legal_guidance.pdf.

184. *Cf. infra* text accompanying notes 190-92.

185. *See* DEPARTMENT FOR CONSTITUTIONAL AFFAIRS, QUESTIONNAIRE FOR MEMBER STATES ON THE IMPLEMENTATION OF DIRECTIVE 95/46/EC, UNITED KINGDOM GOVERNMENT'S RESPONSE (submitted June 14, 2002 & Sept. 13, 2002).

186. COMMISSION OF THE EUROPEAN COMMUNITIES, *supra* note 177, at 7.

The current state of implementation has improved from the writing of this report. Ireland, for example, has since passed a data protection law.[187] However, the Commission's statements on countries' Article 12 subject access concerns still hold true:

> The Commission is not convinced that the implementation of this provision of the Directive is in fact posing serious practical problems. In any case, the number of access requests seems to remain low. The Commission considers the interpretations and guidance provided by national supervisory authorities so far to be wholly reasonable.[188]

Despite the Directive's infancy, it is counterproductive to base the success of the Directive's framework on the current amount of subject access requests without accounting for potential future changes in behavior and practice. In the information age, data has value.[189] Information is a commodity and there are a plethora of reasons for obtaining personal information beyond those associated with the protection of privacy and other fundamental rights, such as maliciously getting back at a former employer.[190]

Beyond blatantly malicious access requests lies a more ambiguous category of requests—*Durant* provides an interesting example of this category. Even though there is no intent element in a subject access request, the court was keen to thwart Durant's "misguided" attempt to obtain discovery through data protection laws because the information was arguably unobtainable through UK discovery rules.[191] The importance of data protection laws is paramount when considering that privacy has

---

187. Data Protection (Amendment) Act, 2003 (Act No. 6/2003) (Ir.), *available at* http://www.dataprivacy.ie/documents/legal/ act2003.pdf (last visited Dec. 20, 2005).

188. COMMISSION OF THE EUROPEAN COMMUNITIES, *supra* note 177, at 15.

189. *See, e.g.*, Jeff Breinholt, *Seeking Synchronicity: Thoughts on the Role of Domestic Law Enforcement in Counterterrorism*, 21 AM. U. INT'L L. REV. 157, 160-61 (2005) (reviewing the importance of "raw information" and the necessity of collecting and using such information to reach an end goal, which, in this case, is obstructing terrorist acts).

190. For example, a disgruntled employee rightfully discharged for some personal impropriety may turn around and request that the organization provide every piece of data in its files "related to" the former employee. Such requests by former employees may certainly be legitimate and situations like this hypothetical have already arisen. *See* DOUWE KORFF, EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE: COMPARATIVE SUMMARY OF NATIONAL LAW 108 (2002). However, this scenario highlights how subject access rights can be used for malicious purposes.

191. Durant v. Financial Services Authority, [2003] EWCA (Civ) 1746, [31].

obtained the status of a human right in Europe,[192] but the use of the subject access provisions to thwart or circumvent other laws and rules warrants further attention and clarification.

Compliance difficulties, the allocation of time and other resources, the future expansion in the use of access rights, malicious uses of access rights by data subjects, and subject access requests that can circumvent other laws are all reasons for reevaluating the subject access provisions in data protection laws. Reevaluation must weigh these issues against a better understood and explained personal data definition. Under Article 13, the Directive explicitly acknowledges the importance of limiting subject access rights under specified circumstances, such as protecting national security interests and performing scientific research.[193] Additional limitations could therefore be imposed within the current structure of the Directive; an action for intentionally withholding information without cause by data controllers would supplement the limiting framework.

VIII. CONCLUSION

Durant's deviation from the Directive framework is unquestionable. As this Article has demonstrated, the fault for these deviations lie with the court, not the underlying statute.

The UK Information Commissioner recognizes the problems caused by *Durant*. Recent efforts to minimize *Durant*'s confusing reasoning through additional guidance is a step in the right direction.[194] However, a few tangible examples outlining situations where data should be considered "personal" will not compensate for the plethora of unique personal data determinations data controllers must make unless there is a baseline understanding of *what* data protection laws are suppose to protect and *how* this gets accomplished. Further absent in the United Kingdom is a cohesive presentation between regulatory guidance and judicial pronouncements.[195] *Durant* directly contradicts many guiding points made by the Information Commissioner.

---

192. *See* Human Rights Convention, *supra* note 38, art. 8.

193. Directive, *supra* note 1, at 42, art. 13. Interestingly, scientific research is only exempt "where there is clearly no risk of breaching the privacy of the data subject," *id.*, a rather optimistic phrase indeed. *Cf. supra* notes 169-70 and accompanying text (arguing against the possibility of a zero percent risk of unanticipated data exposure whenever data processing occurs).

194. *See* INFORMATION COMMISSIONER, *supra* note 183.

195. On the Information Commissioner's web site, the undated legal guidance discussed *supra* note 183 is right next to a link to the court's summary of *Durant* and the significance of its findings. Information Commissioner, http://www.informationcommissioner.gov.uk/eventual.aspx?id=87.

Looming beneath the surface of the court's erroneous statutory interpretation and understanding of privacy rights, however, lies a larger problem warranting attention. The Directive's definition of personal data, which is intentionally broad enough to protect individuals against a penumbra of negative repercussions, gives way to an equally broad data subject access right. The intersection between personal data and access rights needs greater understanding and warrants further consideration. By highlighting the personal data/subject access rights intersection, this Article seeks to pose two challenges. To those skeptical of the need for such a broad definition of personal data, the challenge is developing a framework for a more limited personal data definition that accounts for contextual considerations,[196] as well as accounting for all the variables that a proper privacy assessment necessitates.[197] To proponents of the current personal data definition, the challenge is developing a framework for subject access rights that will account for the vast amount of current and future problems stemming from the sweeping personal data definition.[198]

The Directive and its implementing national laws affect nearly every individual and organization. These effects are not limited to European countries and their constituents.[199] Cross-border information sharing in both the public and private sphere captures an exponentially greater amount of players who will be affected by the requirements of the Directive to varying degree. The lessons of the *Durant* case highlight the need to develop a greater understanding of the personal data definition, and to create a better framework for striking the appropriate balance between personal data and subject access rights while the utilization of Article 12 is low.

196. *See supra* Part VII.A.

197. *See supra* Part VII.B.

198. *See supra* Part VII.C.

199. *See* Directive, *supra* note 1, at 45, art. 25 (regulating the transmission of data to countries outside the European Community).