Global Business & Development Law Journal

Volume 10 | Issue 1 Article 6

1-1-1997

Informed Lending Decisions vs Privacy Interests in Great Britain: Technology over the Edge of Infringement

Robert B. Bale
University of the Pacific, McGeorge School of Law

Informed Lending Decisions vs Privacy Interests in Great Britain: Technology Over the Edge of Infringement

Robert B. Bale*

TABLE OF CONTENTS

---

* J.D., University of the Pacific, McGeorge School of Law, to be conferred 1998; B.S., Arizona State University, 1979. Before law school, I spent over a decade directing the marketing efforts of multi-national retail sales organizations dependent on personal credit information as part of an "informed lending" process. I am grateful to Tim Naprawa and Wendy Green, without whose assistance my dream of publication would have died a'borning. This Comment is dedicated to Mrs. Doris S. Bale: many thanks to a Mom who never stopped believing.

I. INTRODUCTION

Today an individual's ability to obtain housing, purchase goods, qualify for a promotion, purchase insurance, buy a car, or even rent a hotel room depends on that person's creditworthiness.[1] A person with good credit[2] enjoys substantially more financial freedom than a person with poor credit.[3] In Great Britain, third party vendors gather, maintain, package and distribute credit reports about individuals.[4] Errors made by these vendors in an individual's credit report may harm that person.[5] British

---

1. *See* BOARD OF GOVERNORS, FEDERAL RESERVE SYSTEM, CONSUMER HANDBOOK OF CREDIT PROTECTION LAWS (1993) [hereinafter CONSUMER HANDBOOK] (defining creditworthiness as an ability to repay debt and a willingness to do so). Traditional lending criteria evaluate characteristics such as job and residence stability, credit history, and collateral. *Id.* Elements such as income, length of time on the job and credit history are typically given more weight in an equation combining all factors. *Id. See also* FAIR, ISAAC AND COMPANY INC., ANALYZING A CREDIT REPORT: FACTS AND FALLACIES 4-9 (1995) (copy on file with *The Transnational Lawyer*) [hereinafter FACTS AND FALLACIES] (analyzing credit risk as a composite of many different factors including payment history, public record and collection items, outstanding debt, credit history, credit inquiries, trade lines, and the type and mix of credit in use); FAIR, ISAAC AND COMPANY, INC., ANNUAL REPORT 1995 A (1995) (copy on file with *The Transnational Lawyer*) [hereinafter ANNUAL REPORT 1995] (identifying Fair, Isaac and Company Inc. as a leading developer and provider of data management systems and services for the consumer credit industry, ranked first or second in sales of every type of credit management product). The company generated over $113,881,000 in fiscal 1995 revenues providing a variety of credit scoring services. *Id. But see* Peter P. Swire, *The Persistent Problem of Lending Discrimination: A Law and Economics Analysis*, 73 TEX. L. REV. 787 (1995) [hereinafter *Persistent Problem*] (positing certain alternative criteria that might predict credit-worthiness as effectively as existing practices).

2. *See* PAUL B. RASOR, CONSUMER FINANCE LAW 1 (1985) (characterizing credit as a medium of limited acceptance, the use of which depends on factors such as one's credit history, which is independent of how much cash one has); *see also* JOHN KENNETH GAILBRAITH, MONEY, WHENCE IT CAME, WHERE IT WENT 71 (1975) (stating that, "credit allows the man with energy and no money to participate in the economy more or less on a par with the man who has capital of his own").

3. *See supra* note 1 (noting for example that mortgage applicants with past due payments are not likely to qualify for a loan that would otherwise be granted); *see also* FACTS AND FALLACIES, *supra* note 1, at 14 (identifying as high risk a credit profile showing one thirty-day delinquency, and exhibiting higher than desirable ratios of cash balances to credit). This example of a credit profile which would be denied credit is presented in a booklet distributed by Fair, Isaac to lenders for the purpose of teaching how to evaluate loan candidates. *Id.*

4. OFFICE OF FAIR TRADING, KNOW YOUR RIGHTS 2, 8 (1994) [hereinafter KNOW YOUR RIGHTS] (identifying the top three British credit reporting agencies as CCN Group Ltd, Credit and Data Marketing Services, and Equifax Europe). The Office of Fair Trading monitors credit transactions in England. *Id.*

5. *See* DONNA NOEL, CREDIT SURVIVAL GUIDE 25 (ICF & Success Seminars eds., 1995) [hereinafter CREDIT SURVIVAL GUIDE] (asserting credit ratings directly impact a wide range of factors, including one's residence, interest rates charged for installment purchases, ability to travel, rent a car or stay in a hotel, the amount of

statutes requiring accuracy protect certain categories of personal information.[6] Unfortunately, a practical application of these statutes does not allow individuals to recover for damages caused by inaccuracies in their personal databases.[7] This Comment explores the harm to individual privacy rights caused by informational errors.

Great Britain seeks to learn from equivocation in U.S. data protection laws[8] by narrowly defining a protected right to informational privacy.[9] Britain emphasizes the relationship between private information and its dissemination in a commercial context.[10] Less opportunity for ambiguity exists in determining whether a privacy right has been violated when those rights are narrowly defined.[11] Rationally, transgression is less likely to occur when it is easier to detect a violation.[12] But companies which compile personal information manage massive amounts of data.[13] Recent technological breakthroughs[14] have made it easy for these companies to combine infor-

---

fees and points paid when purchasing a home, and employment or job promotions). Specifically, those with poor credit pay higher interest rates than borrowers with good credit; the people who can least afford credit pay the most for it. *Id. See, e.g.*, AL GRIFFIN, THE CREDIT JUNGLE 121-22 (1971) (noting that persons denied traditional forms of credit often seek it at a higher cost from neighborhood finance companies, loan sharks, etc., thus driving up the cost of credit to those individuals least able to afford it).

6. *See generally* Data Protection Act 1984, part I, §§ 2-3, *reprinted in* 6 HALBURY'S LAWS OF ENGLAND AND WALES 902-03 (4th ed. 1992) [hereinafter DPA] (enabling protection of personal information which relates to a living individual who can be identified from that information, and which is recorded in a form in which it can be processed electronically by equipment operating in response to instructions).

7. *See infra* notes 299-320 and accompanying text (discussing the barriers to recovery facing private individuals harmed by inaccurate personal data).

8. Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 437 (1995) [hereinafter *Information Privacy*] (reviewing the European Union's concern that inadequate data protection in the United States will ultimately result in a prohibition of data transfers between the U.S. and member nations); Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?* 44 FED. COM. L.J. 195, 196 (1992) [hereinafter *Privacy in the Information Economy*] (reporting on federally mandated studies extending back 20 years, which conclude that privacy in the United States is not adequately protected from either government or industry intrusions). Reidenberg asserts that existing federal and state frameworks for the legal protection of individual rights are too meager in scope, application and statutory protection to serve the interests of a concerned public. *Id.* at 200.

9. *See supra* note 6 (noting how the primary statutory authority defines privacy rights in terms of personal data). Philosophically, this Comment follows Westin's definition of privacy. *See* ALAN WESTIN, PRIVACY AND FREEDOM 7 (1970) (defining a protected privacy interest as the right to control information about oneself).

10. Elizabeth France, *Data Protection Act*, Office of the Data Registrar Home Page, <http://www.open.gov.uk/dpr/dprhome.htm> (visited Oct. 25, 1996) (copy on file with *The Transnational Lawyer*) (emphasizing that the Data Protection Act focuses on the electronic processing and dissemination of information about living, identifiable human beings, whether sensitive or not).

11. DPA, *supra* note 6, part I, § 1(1)-(3) (defining personal interests in terms of data about a specific individual which can be gathered, stored and disseminated by another entity).

12. *See* Jennifer L. Kraus, Note, *On the Regulation of Personal Data Flows in Europe and the United States*, 1993 COLUM. BUS. L. REV. 59, 66 (1993) [hereinafter *Regulation of Personal Data Flows*] (postulating that individual European countries, including the United Kingdom, have structured narrow laws intended to restrict access to data to address problems of intrusiveness, inaccuracies and competition).

13. *See infra* notes 62-64 and accompanying text (describing the enormous volume of personal data processed by commercial data gatherers).

14. *See infra* notes 64-73 and accompanying text (relating technological advances in compiling personal information databases).

mation from many different databases.[15] This information is valuable to retailers, commercial lenders, banks, marketing groups, or any other party which directly or indirectly sells something.[16] The pragmatic application of readily-available information technology allows efficient gathering, processing, manipulating and delivery of this valuable personal data.[17] Conversely, some regard this technology as an uncontrollable juggernaut inevitably destined to infringe on protected privacy interests.[18]

The European Union reached the conclusion that privacy rights needed protection over a decade ago, and responded by formulating regulations governing inter-country transfers of personal data.[19] These regulations require member nations to erect statutory protections of personal data.[20] Members may only transfer personal

---

15. *See infra* note 66 and accompanying text (discussing the ways in which commercial data gatherers combine information from across a wide variety of data platforms).

16. *See infra* notes 65-77 and accompanying text (defining the types of businesses that depend on and seek out personal data).

17. *See infra* notes 62-73 and accompanying text (reviewing personal data accumulation strategies).

18. *See* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 554 (1995) [hereinafter *Privacy and Participation*] (asserting that global information sharing renders the protection of individual privacy a "critical regulatory challenge"); *see also* Paul M. Schwartz, *Symposium: Data Protection Law and the European Union's Directive: The Challenge for the United States*, 80 IOWA L. REV. 471 (1995) [hereinafter *Challenge for the United States*] (relating the control of information on the Information Superhighway to compelling issues of power, legal rules, industry norms, business practices, and economic impact, which are at the forefront of "policy discussions among businesses, governments, and citizens"); Michael P. Roch, *Articles: Filling the Void of Data Protection in the United States: Following the European Example*, 12 COMPUTER & HIGH TECH. L.J. 71, 71 (1995) (describing the growth of business and government reliance on computer technology for record keeping, market analysis, managerial decisions, census data, and intelligence purposes over the past two decades, to the inevitable accumulation of information about private citizens in either a government or commercial database, at a minimum); Sari Kalin, *News Analysis Deregulation of Foreign Internet Access Costs Soar Above United States'*, INFO. WORLD, Oct. 28, 1996 at *1, *available in* 1996 WL 12273178 (reporting on estimates that the rapid growth of Internet activity will result in more than 100 million users by the end of 1998); John A. Quelch & Lisa R. Klein, *The Internet and International Marketing*, SLOAN MGMT. REV., Mar. 1, 1996 at *1, *available in* 1996 WL 10054575 (asserting that the current expansion of Internet use is fueled by marketing efforts to provide products and information to potential buyers); Stephen P. Aranoff, *Browsing the Web for Profit Potential*, GRAPHIC ARTS MONTHLY., July 1, 1996, at *2, *available in* 1996 WL 8735117 [hereinafter *Browsing the Web*] (interviewing David Scott Carlick, senior vice president of advertising firm Poppe, Tyson). Carlick states that one of the primary reasons Internet advertising continues to grow is its ability to lower the cost of generating new customer leads, and consequently, the cost of making a sale. *Id.*

19. *See Challenge for the United States*, *supra* note 18, at 474 (reviewing the efforts made by the Council of Europe and Commission of the European Union, on behalf of member nations including the United Kingdom to address the issue of international data transfers). Schwartz notes that the legal solutions allow blockage of data transfers to countries with insufficient internal protection of privacy interests. *Id.* He suggests such measures may actually challenge the free flow of data to the United States. *Id.*

20. *See generally Information Privacy*, *supra* note 8 (differentiating between privacy guidelines issued by the Committee of Ministers of the Organization for Economic Cooperate and Development, and conventions for the Protection of Individuals with Regard to Automatic Processing of Personal Data promulgated by the Council of Europe). The guidelines represent basic principles for data protection and the free flow of information among countries with laws conforming to the protection principles, but are without the force of law. *Id.* at 431. But, the Council of Europe requires countries wishing to engage in the transborder exchange of personal data to enact conforming national laws. *Id.* at 431-32. *See also id.* at 432 (reporting that as a result of the disparities between

data to countries in compliance with European Union standards.[21] Though the United Kingdom's passage of data protection laws in 1984[22] makes Britain a relative newcomer to the arena of data protection,[23] commentators generally regard Britain's data protection provisions as consistent with the standards required by the Union.[24] But these statutes work better on paper than in practice.[25] Industry foot dragging is part of the problem; barely half the companies required to register as users of personal data have done so.[26] Also, while the nation's data protection laws compel correction of inaccurate personal information,[27] damages caused by inaccuracies in that information are inaccessible to the individuals harmed.[28]

This Comment focuses on the data protection statute intended to safeguard personal information from infringement by businesses granting consumer credit.[29] Part II defines the relevant terminology, and discusses the heightened threat to privacy interests represented by information technology within a commercial context.[30] Additionally, Part II reviews the impact of modern technology on efforts to protect

---

various approaches, the Commission of the European Community drafted an ambitious Council Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data). Cate characterizes the Directive as extraordinary comprehensive, and notes it requires each of the member states to enact laws governing the processing of personal data. *Id.* at 433. The law must guarantee certain basic protections, including data processing which is accurate, up-to-date, relevant and not excessive. *Id.* Further, data may not be kept for longer than necessary to achieve the purpose for which it was gathered, and may only be collected and used for legitimate purposes. *Id.*

21. *Id.*

22. *See generally* DPA, *supra* note 6 (applying statutory authority over data protection to England, Wales and Ireland). This omnibus legislation was passed in 1984. *Id.*

23. *See Filling the Void of Data Protection in the United States: Following the European Example*, *supra* note 18, at 76-77 (recognizing Sweden and Germany as the first member nations to pass laws intended to protect personal privacy). Sweden passed its first national data protection laws in 1973, and Germany began its long-standing tradition of privacy in the German Civil Code of 1896. *Id.*

24. *See* Joel R. Reidenberg, *The Privacy Obstacle Course: Hurdling Barriers to Transnational Financial Services*, 60 FORDHAM L. REV. 137, 148 (1992) [hereinafter *Privacy Obstacle Course*] (characterizing the United Kingdom's omnibus Data Protection Act as consistent with the broad data protection stipulations in the European Convention); Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471, 474 (1995) [hereinafter *Restrictions on Data Flows*] (noting Great Britain forbids the transfer of any data likely to contravene the data protection principles expressed by the European Union).

25. *See infra* notes 282-84 and accompanying text (criticizing the failure of Britain's primary authority to adequately protect consumers harmed by inaccurate data because of ill-defined regulatory provisions and statutory defenses favoring commercial interests).

26. *See infra* note 187 and accompanying text (reporting on the lack of compliance with registration requirements under the Data Protection Act of 1984).

27. DPA, *supra* note 6, part III, § 24(1) (granting judicial authority to compel the rectification or erasure of personal data on a determination that the data is inaccurate).

28. *See infra* notes 299-320 and accompanying text (denoting the challenges faced by consumers seeking recovery for damages caused by inaccurate personal data).

29. *See generally* DPA, *supra* note 6.

30. *See infra* notes 76-77, 167-68 and accompanying text (regarding the threat to privacy interests inherent in advancing information technology, especially problematic in the area of credit transactions).

privacy rights.[31] Part III distinguishes the interests of private individuals,[32] companies which harvest information about those individuals,[33] and lenders who use that information in credit transactions.[34] It then examines the conflicts and common grounds between those interests.[35] Part IV discusses Britain's legislative solution to infringement through an analysis of the primary authority[36] protecting personal data, including a review of available remedies.[37] The section identifies potential barriers to successful government monitoring of commercial data users and prosecution of data protection violators.[38] Part V posits four proposals to heighten protection of personal data by achieving a more equitable balance between privacy interests and legitimate commercial concerns.[39] Part VI concludes that a balance can be struck between commercial and private interests by shifting the burden for insuring data accuracy, modifying statutory defenses to promote greater chances of recovery by harmed individuals, and allowing disinterested individuals to opt out of electronic databases.

II. OVERVIEW

This section begins by defining relevant terms, then proceeds to a brief overview of Britain's legislative attempts to protect private data. Next discussed is the corrosive impact of information technology on privacy rights in general. A hypothetical example illustrates the problems faced by a typical consumer who suffers damage because of improper data management. Finally, the Comment scrutinizes injuries to privacy rights within the context of a commercial lending transaction.

---

31. *See id.*

32. *See infra* note 60 and accompanying text (defining private interests).

33. *See infra* notes 174-76 and accompanying text (defining the interests of commercial gatherers of personal information).

34. *See infra* notes 192-99 and accompanying text (defining interests of commercial lenders).

35. *See infra* notes 212-21 and accompanying text (identifying the intersection of commercial and private interests).

36. *See generally* DPA, *supra* note 6.

37. *See infra* notes 300-06 and accompanying text (reviewing the practical reality of access to statutory relief).

38. *See infra* notes 307-13 and accompanying text (criticizing the ease with which businesses can avoid liability for harm caused to consumers by inaccurate databases); *see also infra* note 148 and accompanying text (reporting the government's failure to compel registration of data users for regulatory purposes).

39. *See infra* notes 334-55 and accompanying text (exploring alternatives to protecting important privacy interests without prohibiting legitimate commercial activities).

A. *Definition of Terms*

Data[40] refers to information recorded in a form in which it can be automatically processed by computer equipment in response to specific instructions.[41] Similarly, personal data is a subset of data which relates to a living individual who can be identified by virtue of that information.[42] Relatedly, a data subject is an individual about whom personal information is stored in a database due to third party efforts.[43] Data gatherer refers to any person or entity which gathers, amends, augments, deletes, and rearranges personal data or information extracted from or added to a data subject's file.[44] Gatherers may provide other parties with services by processing or allowing another party to process the information it holds.[45] Conversely, a data user relies on information from data gatherers to assist in evaluating the risks associated with granting some form of credit.[46] Now that basic terms have been defined, the following section discusses British efforts to provide statutory protection of personal data.

B. *Background*

British efforts to provide statutory protection of personal data mirror the historical abhorrence of unwanted intrusions on personal liberty seen in other advanced nations.[47] The roots of British law extend back to the Magna Carta,[48] which placed individual liberties above all others except communal rights, a concept adopted by British common law in the thirteenth century.[49] Today, the nation protects personal data through two broad consumer protection acts,[50] the latter of which is the focus of this Comment.

---

40. THE NEW WEBSTER ENCYCLOPEDIC DICTIONARY 217 (1971) (defining datum as "some fact, proposition, quantity or condition granted or known from which other facts are to be deduced"). The terms "data" and "datum" will be used interchangeably throughout this Comment.

41. DPA, *supra* note 6, part I, § 1(2).

42. *Id.* part I, § 1(3).

43. *Id.* part I, § 1(4).

44. *See id.* part I, § 1(6) (defining credit bureau). This Comment adopts the term "data gatherer" and uses it interchangeably with "credit bureau."

45. *Id.*

46. *Id.* part I, § 1(5)(a)-(c).

47. *Cf., e.g.,* U.S. CONST. amends. IV ("The right of the people to be secure in their persons. . . shall not be violated"); *id.* V ("No person shall. . . be deprived of life, liberty or property without due process of law"); *id.* XIV, §1 ("[N]o state shall make or enforce any law which shall abridge the privileges and immunities of citizens. . ."). *See Privacy and Participation, supra* note 18, at 566 (framing the Constitutional argument favoring protection of informational privacy); *see also, e.g., Filling the Void of Data Protection in the United States: Following the European Example, supra* note 18, at 77 (reporting Germany's passage of the first data protection laws in the late 1800's).

48. Mark Allan Gray, *The International Crime of Ecocide,* 215 CAL. W. INT'L. L.J. 30 (1996).

49. *Id.*

50. *E.g.,* Consumer Credit Act 1974, *reprinted in* 11 HALSBURY'S STATUTES OF ENGLAND AND WALES 15 (4th ed. 1991) [hereinafter CCA]; DPA *supra* note 6.

In order to afford the consumer consistent and comprehensive protection of the right to privacy across the whole spectrum of credit transactions, the Consumer Credit Act[51] (CCA) standardized statutory treatment of all the different branches of the credit industry under one code.[52] This consolidated previous legislative attempts which offered piecemeal regulation of various credit transactions.[53] The CCA offers broad shelter for the majority of consumer credit transactions,[54] but does not protect the integrity of personal data.[55]

The narrower Data Protection Act[56] (DPA) recognizes increasing challenges to personal liberty presented by electronic data processing, and establishes comprehensive provisions guiding the collection, management and dissemination of private data.[57] The Act aims at protecting any discrete personal information[58] which can be electronically processed, regardless of its sensitivity.[59] Commercial encroachment on this information[60] leads to the erosion of privacy interests.

1. *The Erosion of Privacy Interests*

This Comment regards a privacy interests as the right of an individual to maintain the integrity of any personal information gathered about that individual.[61] Yet, this desire for information autonomy conflicts with the expansion of technology

---

51. CCA, *supra* note 50.

52. *See* CCA, *supra* note 50, part I, § 1(1).

53. *See* 22 HALBURY'S LAWS OF ENGLAND, para. 1, at 3 (4th ed. 1979) (tracing the development of hire-purchase legislation from the Money-lenders Act 1900, and including the Pawnbrokers Act 1872, through the Hire-Purchase Acts of 1938, 1954 and 1964).

54. *See id.* at 6 (noting the Act only applies to agreements involving less than £5000, or approximately US$12,500).

55. *See* CCA, *supra* note 50, part II, § 159(1)-(4) (detailing the statutory steps available to consumers who detect inaccuracies in their credit report). Data gatherers are not compelled to insure or maintain the integrity of personal information under this Act. *Id.*

56. *See generally* DPA, *supra* note 6 (failing to directly monitor or regulate credit transactions, but providing for damages when consumers are harmed by inaccurate data).

57. DPA, *supra* note 6, sched. 1, part 1 (expressing the eight data protection principles intended as provide broad protection to personal data subject to electronic processing).

58. *See* Elizabeth France, *What Does the Act Cover?*, Office of the Data Registrar Home Page, <http://www.open.gov.uk/dpr/dprhome.htm> (visited Nov. 5, 1996) (copy on file with *The Transnational Lawyer*) (explaining the Act is concerned with any personal data about a living, identifiable individual, which is subject to automatic processing, including merely their name and address).

59. *Id.*

60. *See generally infra* notes 63-78 and accompanying text (portraying the myriad ways individual privacy rights are threatened by information technology).

61. Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 498 (1995) [hereinafter *Setting Standards*] (applying this standard to fair information practices). This Comment follows Reidenberg by applying these standards to the collection, storage, use and disclosure of personal information. *Id. See* Deborah Hagan, *Credit Reporting and Privacy Issues*, 80 ILL. B.J. 412, 415 (1992) (identifying the right to control information about oneself as one of the most important attributes of a right to privacy); *cf. id.* (asserting the consumer wishing to live in a credit-based society must trade off a portion of his or her privacy).

dedicated to managing information markets.[62] The advent of data warehouses[63] which accumulate vast hoards of personal information from an ever-expanding variety of sources[64] has turned information management into an art form.[65]

---

62. Alan D. Fischer, *Author Shares Tips on Marketing on the Net*, ARIZ. DLY. STAR, June 16, 1995, at 4B (interviewing Charles Rubin, author of GUERRILLA MARKETING ONLINE). Rubin stated Web pages could now be constructed for as little as $20 per page, and characterized Internet marketing as cost-effective, and bound to increase in value. *Id.*; *see* Quelch & Klein, *supra* note 18 (reporting nations like the United States, the United Kingdom, Denmark, Finland, and Belgium saw the number of domestic Internet hosts increase by a minimum of 100% in 1995 alone; New Zealand's hosts increased by nearly 450% in the same period).

63. *See* ANNUAL REPORT 1995, *supra* note 1 (reporting 1995 revenues of US$113,881,000 from providing global database management services); *see also* John Goss, *"We Know Who You Are and We Know Where You Live": The Instrumental Rationality of Geodemographic Systems*, ECON. GEOGRAPHY., Apr. 1, 1995, at *7, *available in* 1995 WL 12232272 [hereinafter *Instrumental Rationality*] (setting forth various examples of large scale data warehouses). Goss regards Claritas, Inc.'s processing of data from credit bureau files, car ownership, banks, census records, purchasing surveys, and other public and private services on over one-hundred million U.S. households; R.L. Polk's Totalist, controlling information on 95% of all U.S. households as a result of combining information from over 20 separate data banks; and NDS's Lifestyle Network, which offers marketing clients a huge, unique database compiled from customized consumer surveys. *Id*; *see also* Amy Fleischmann, *Personal Data Security: Divergent Standards in the European Union and the United States*, 19 FORDHAM INT'L L.J. 143, 143 (1995) (declaring the growing dependence of industry on information systems and the amount of personal data processed is approaching staggering proportions); *id.* at 143 n.3 (reporting that Solomon Brothers trades in the trillions in securities and an equivalent of total U.S. bank holdings through its computer networks annually); *Law: All Trade Deals Revolve Around the Exchange of Products and Information*, EUROMONEY TRADE FIN. & BANKER INT'L, Sept. 28, 1987, *available in* LEXIS, Reuter Textline [hereinafter *All Trade Deals*] (reporting nearly a decade ago the use of data transfers by British exporters increased 250% between 1986 and 1988, and quoting industry expert predictions that ICL, a British data processing firm, would sign up over 100,000 data users by the year 2000). *See infra* note 78 (reporting American Express' gold mine of personal data). This Comment also notes data mining through 'massively parallel' supercomputers capable of collating, breaking down and cross-referencing vast amounts of data from hundreds of sources in minutes. *Id. See also Master the Internet Kotler Tells Marketing Profession*, CHARTERED INST. OF MKTG., Oct. 7, 1996, at *1, *available on* WL 1996 13546786 (quoting marketing guru Professor Philip Kotler addressing an audience of London marketing executives). Kotler advised that to remain competitive, companies must master database marketing to provide consumers with an alternative to traditional store-based retailing. *Id. See also* Kathleen A. Linert, *Database Marketing and Personal Privacy in the Information Age*, 18 SUFFOLK TRANSNAT'L L. REV. 687, 690 (1995) (relating the existence of one million databased mailing lists in the United States alone, including lists of new households, businesses, professionals, graduates, institutions, babies, marriages, credit card holders, and automobile registrants). Linert explains how personal information can be scrutinized by anyone with a personal computer just by tapping into thousands of available databases. *Id.* at 687. *But see The Europeans Take a Hard Line on Data Privacy*, CREDIT CARD NEWS, Apr. 1, 1996, at *1, *available in* 1996 WL 8385684 [hereinafter *Hard Line on Data Privacy*] (reporting the difficulties faced by British credit card issuers in building solicitation databases because of strict privacy laws).

64. A. Michael Froomkin, *Regulation and Computing and Information Technology: Flood Control on the Database Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 J. L. & COM. 395, 480 (1996) [hereinafter *Flood Control*] (reporting that the most important part of the emerging database phenomenon relates to the growth of computer processing power in terms of expanded technological abilities to cross-reference multiple, extensive databases across commercial, law-enforcement and medical boundaries as part of a "routine" personal data collection effort); *see, e.g., Privacy and Participation*, *supra* note 18, at 612 (noting that the "majority of states have traditionally released motor vehicle registration and driver license information"). *See generally supra* note 63.

65. For example, today's global shoe salesperson can pitch a new line of women's pumps directly to every single, professional woman between the age of 30 and 45 who weighs more than 135 pounds, earns over $32,000 per year, adores the color blue, vacationed out of her nation of residence at least once in the past five years, drives a German auto and lives in Chicago, Paris or London. *See generally supra* note 63 (reviewing the prevalence of

Applying this technology, companies can target specific audiences. This ability to focus marketing efforts does not depend upon feedback or even cooperation from potential customers.[66] Every tidbit of relevant information is uncovered along the electronic paper trails left by practically every modern consumer.[67] Virtually every financial transaction may be compiled, manipulated and analyzed.[68] For example, discrete individual data ranging from the type of dessert ordered at lunch,[69] the books read,[70] gifts bought,[71] or home mortgaged[72] can be gathered and consolidated as part of a gigantic database.[73] While access to this information may benefit commercial interests through increased marketing efficiency,[74] some commentators believe its mere existence may lead to a degradation of personal privacy rights, even if allowed to remain dormant.[75] But personal information is far from dormant; industry depends

---

large-scale data accumulation); *supra* note 64 (discussing network technology's ability to cross-reference multiple, extensive databases across numerous platforms).

66. *Flood Control, supra* note 64, at 479-480 (declaring that personal privacy has been negatively affected by the "revolution in data acquisition, processing and storage). Froomkin represents that every transaction on the World Wide Web, including retail sales and information captured as a result of an on-line transaction of any kind, is subject to recording and archiving. *Id.* at 480. He draws a parallel to similar innovations in the public arena (e.g., day-to-day transactions at point-of-purchase, in courtrooms, or at medical centers), and observes that the ability to access and combine these databases leaves the average citizen with little in the way of personal privacy. *Id.* at 479-480. Companies are not above soliciting personal information directly from consumers; recently the author received an invitation by mail from AT&T phone company offering lower long distance rates in exchange for permission to distribute information about the author to other commercial entities. *See Regulation of Personal Data Flows, supra* note 12, at 61 (describing the 'relative ease' with which exhaustive databases on enormous numbers of people can be compiled). For example, personal database entries occur when an individual calls an 800 number, cashes a coupon, fills out a warranty card, subscribes to a magazine, or books a hotel room. *Id.*

67. *See Flood Control, supra* note 64.

68. *Id.*

69. *See id.*; *see also Instrumental Rationality, supra* note 63 (critiquing geodemographic systems, sophisticated marketing tools responsible for a revolution in marketing research). These systems combine massive electronic databases on consumer characteristics and behavior and applies the information to exercise rational knowledge-based control over consumer buying decisions. *Id.* Goss hypothesizes this type of power may one day be used to force individuals into buying choices. *Id.*

70. *Flood Control, supra* note 64.

71. *Id.*

72. *See* RASOR, *supra* note 2, at 18 (noting that credit reports include public record information including tax and other liens).

73. *See generally supra* notes 64-72 and accompanying text (explaining information technology's ability to accumulate and manage information).

74. *See infra* notes 113-24 and accompanying text (discussing the various ways information technology has lowered costs and increased marketing efficiency).

75. ORRIN KLAPP, OVERLOAD AND BOREDOM: ESSAYS ON THE QUALITY OF LIFE IN THE INFORMATION SOCIETY 2-3 (1986) [hereinafter OVERLOAD] (explaining how matter and energy naturally degrade to more random, less ordered states). In terms of information entropy theory, the larger the amounts of information processed or diffused, the more likely it is that information will degrade towards meaningless variety, like noise or information overload. *Id.* In statistical terms, information theory entropy suggests that the mere presence of stockpiled information increases the likelihood of its breakdown, disintegration and disorganization, leading by inference to an infringement on personal privacy rights. *Id.* Klapp's analysis has special application within the context of large-scale data processing, which he theorizes is inherently problematic in terms of maintaining information integrity. *See id.* He speculates "[T]he more information is repeated and duplicated... the more kinds of media through which

upon it, seeks it out, buys it, and manipulates it.[76] Thus, information technology degrades privacy rights[77] at the same time it increases commercial productivity.[78] When privacy rights are so degraded that individual liberties are harmed[79] this becomes problematic.

British citizens wishing to protect privacy rights face two problems. First, information technology gives businesses access to personal data, whether or not the individual consumer who is the subject of that data desires such access.[80] Second,

---

information is passed, the more decoding and encoding, and so on—the more degraded information might be." *Id* at 126.

76. *See Privacy in the Information Economy*, *supra* note 8, at 197 (maintaining that the proliferation of computers has encouraged commercial use of sophisticated data collection strategies involving information service providers and data clearinghouses; interconnected computing systems and expanded processing abilities have resulted in diminished responsibility for the protection of personal information, as evidenced by the decreased contacts between individuals and those holding personal data). Reidenberg points to the "vast quantities of personal information containing greater detail than ever before about an individual's financial status, health status, activities and personal associations," now readily available through commercial data gatherers. *Id.* at 198. As to commerce's reliance on this information, Redienberg points out the reciprocal marketing of personal databases is now estimated to be a three billion dollar industry. *Id.* (citing Jill Smolowe, *Read This!!!!!!*, TIME, Nov. 26, 1990, at 62, 66). *See generally supra* notes 62-73 (reviewing large scale personal information managers).

77. For examples of what happens when personal information is not properly managed, see Karen Epper, *Crime Watch: Credit Bureaus Step Up Their Efforts Against Data Fraud*, AM. BANKER., Dec. 14, 1993, at *1, *available in* 1993 WL 5853014 (reporting the arrest of 15 auto dealer employees for using personal data obtained from credit reports to fraudulently gain cash and credit lines). *See Regulation of Personal Data Flows*, *supra* note 12, at 62 (relating the experience of Mr. and Mrs. Michael Riley, who, after experiencing a problem with a pre-approved credit card, were told by their bank that their car had been repossessed, they faced $70,000 in tax liens, and that they had filed for bankruptcy; the lender had purchased inaccurate information from a data warehouse, which confused Michael George with Michael Gilbert Riley); *see also* Lisa Fickenscher, *Credit Industry Strains to Stem Tide of Identity Theft*, Oct. 24, 1996 at *1, *available in* 1996 WL 5568880 (quoting Dennis Rice, director of compliance and fraud control services for Experian Inc., formerly TRW). Identity theft occurs when an individual's private data is stolen from electronic databases and used to impersonate that individual for the purpose of obtaining credit. *Id.* According to Rice, "The problem [of identity theft] has increased so much that . . . it is putting a strain on all our systems to keep up with it." *Id.*

78. *See* Laurie Hays, *Using Computers to Divine Who Might Buy a Gas Grill*, WALL ST. J., Aug. 16, 1994, at *1, *available in* 1994 WL-WSJ 340727 [hereinafter *Using Computers to Divine*] (reporting that American Express accumulated more than 500 billion bytes of data analyzing how customers used 35 million charge cards to charge US$350 billion in credit card purchases between 1991 and 1994); *Flood Control*, *supra* note 64, at 486 (discussing the practice of "data mining" by companies intent on identifying client preferences, purchase and credit histories with regards to maintaining the client as a happy customer).

79. This Comment contends that commercial interests have superseded individual privacy rights in Great Britain. *See, e.g.*, *supra* notes 76-77.

80. *See generally* DPA, *supra* note 6, sched. I, part 1 (setting forth the data protection principles; while the Act circumscribes the purposes for which data can be held, the parties who can acquire and receive it, and compels correctness, a private individual may not prevent collection of accurate personal data to be used for legitimate purposes). *But see Regulation of Personal Data Flows*, *supra* note 12, at 71 (referring to European directive provisions adopted by the United Kingdom and Great Britain allowing private individuals to object to processing of personal information when that data is intended for transborder transfers of information). Companies must expressly offer private individuals the opportunity to opt out of any lists offered for such purposes. *Id.*

errors are inevitable in any setting requiring the manipulation of large databases.[81] The following hypothetical examples illustrates this point.

2. *A Hypothetical Example of Harm to Privacy Interests*

When a private citizen is denied credit[82] or is penalized by higher costs to obtain credit[83] due to inaccurate personal data,[84] privacy interests are harmed. While Britain has taken steps to provide a less convoluted litigation remedy than the complex statutory scheme adopted by the United States,[85] this simplified approach[86] to statutory redress of intrusions on privacy rights[87] does not effectively balance commercial and privacy interests. On the one hand, data gatherers who compile quantities of infor-

81. *Regulation of Personal Data Flows*, *supra* note 12, at 62 (relating that 35% of people who pay to receive a copy of their credit report find that someone else's credit history has been mistakenly attributed to them, sometimes with dire consequences); CREDIT SURVIVAL GUIDE, *supra* note 5, at 1 (reporting approximately 1.5 million inquiries are processed each day by the three largest data warehouses in the U.S., and citing studies finding errors in nearly one-half of all reports on file); *see also* OVERLOAD, *supra* note 75, at 2-3 (explaining the natural degradation of matter and energy into random, disordered states).

82. *See generally supra* note 1 (defining creditworthiness and the importance of credit reports in lender credit decisions); *see also* CREDIT SURVIVAL GUIDE, *supra* note 5, at 1 (relating credit is denied to 15% of all applicants as a result of inaccurate personal data).

83. *See Policy Statement on Discrimination in Lending, Federal Interagency Task Force on Fair Lending*, 59 Fed. Reg. 18,268 (1994) [hereinafter *Policy Statement*] (describing how lenders vary the terms of credit, including amount, interest rate, duration or type of loan depending on an applicant's credit score or history); *Don't Get Caught in a HMDA Trap*, A.B.A. BANKING J., Oct. 1991, at 28 (noting that lenders justify differences in terms as a function of risk; those borrowers with good credit constitute less risk than those without).

84. Other injuries which may occur as a result of inaccurate credit reports such as affronts to dignity and psychological damages are beyond the scope of this Comment.

85. For example, citizens in the United States who experience harm due to a perceived invasion or misuse of personal data must select from an extensive variety of statutory, regulatory, and administrative options to seek relief. *See, e.g.*, Fair Credit Billing Act of 1974, 15 U.S.C. § 1666 (1988); Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681t (1988); Fair Debt Collection Practices Act of 1977, 15 U.S.C. §§ 1692b(2), 1692c(b); Equal Credit Opportunity Act of 1974, 15 U.S.C. §§ 1691b(2), 1691c(b) (1988); Electronic Funds Transfer Act of 1978, 15 U.S.C. §§ 1693-1693r (1988); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2520, 2701-2709 (1988); Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-2711 (1988); Family Education Rights and Privacy Act of 1974, 20 U.S.C. § 1232g(b)(1); Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001-2009. Unfortunately, this daunting plethora of remedial alternatives offers little in the way of practical relief. *See Information Privacy*, *supra* note 8, at 437 (noting that the numerous federal statutes intended to safeguard individual privacy interests of U.S. citizens actually offer little in the way of protection).

86. Harm caused by a misuse of data is actionable under either the DPA or CCA. The DPA addresses privacy infringements as to data "recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose." *See* DPA, *supra* note 6, part I, § 1(2). The CCA regulates all manners and forms involved in the granting of "a loan or any other form of financial transaction." *See* CCA, *supra* note 50, part I, § 9(1); *cf. supra* note 85 (suggesting the difficulties faced by United States citizens, who must select from a wide variety of competing and sometimes duplicative statutory, regulatory and administrative acts.

87. *See generally infra* notes 298-99 and accompanying text (describing the primary rights and relief available to consumers harmed by inaccurate personal data).

mation are rewarded[88] and insuring the accuracy of information is not compelled.[89] On the other hand, the private individual must detect inaccuracies and take the proper steps to obtain corrections.[90] A hypothetical example portrays the barriers facing a consumer harmed by inaccurate personal data.

At the age of twenty-seven, John E. Brown[91] was denied credit when Infolink, one of Britain's largest data warehouses,[92] supplied inaccurate data to his mortgage lender. Mr. Brown, an apartment resident for six years, had offered to buy a small house in foreclosure. The house was reduced to a bargain price for quick sale. Brown's £42,000 offer was accepted, and he tendered a ten percent down payment.[93] Brown's application was denied due to poor credit. The mortgage lender relied on a credit scoring system[94] based on data from Infolink. Infolink erroneously attributed negative information about a John A. Brown to John E. Brown's database. In fact, John E. Brown had successfully paid off or maintained a variety of consumer loans and had no adverse credit.

---

88. *See generally infra* notes 174-75 and accompanying text (relating the manner in which data gatherers generate revenue).

89. *See generally infra* note 102 and accompanying text (relating the statutory duty of data users to correct data upon notification of its inaccuracy). *But see infra* notes 273-74 and accompanying text (noting that a data user commits no criminal offense by failing to correct inaccurate personal information).

90. *See infra* note 262 and accompanying text (reviewing DPA's requirements that data subjects detect inaccuracies and expressly notify data users of the need to correct before any remedial action is taken).

91. A hypothetical based on procedures outlined in substantive U.K. law is necessary, since no single case has to date been successfully prosecuted under the DPA on this issue.

92. Sarah Aryanpur, *Special Report - Data Protection - Credit Where Credit's Due*, COMPUTER WKLY., July 15, 1993, *available in* LEXIS, Reuter Textline [hereinafter *Credit Where Credit's Due*].

93. In the hypothetical, the home was priced £5000 below market.

94. *See* ANNUAL REPORT 1995, *supra* note 1, at 8 (explaining the process by which credit scores are calculated). This global provider of data management and credit scoring systems characterizes credit scores as snapshots summing up a person's likely future credit performance at a given point in time. *Id.* The scores are calculated according to mathematical tables that assign points for different bits of information regarded as determinative of future credit performance. *Id.* Fair, Isaac offers lenders assistance in developing a custom scorecard from that lender's own data on its customers. *Id.* This data can either be pooled with information from other databases or isolated to broaden or narrow the score's predictive value. *Id.* Each scorecard consists of information like repayment trends, the amount of credit an individual has, the ages and amounts of various credit lines, loans or cards, recent inquiries that indicate an individual has been shopping for credit, and public record information. *Id.* at 9. Scores give lenders a fast but reliable idea of how likely it is that a particular loan applicant will perform. *Id.* There is strong support in the lending industry for the use of credit scores. *See* Niles S. Campbell, *Credit Scoring Impact on Industry Subject of Concern for GSE Regulator*, BNA BANKING REPORT, Apr. 15, 1996, at 630-631 [hereinafter *Credit Scoring Impact*] (reporting efforts of Fannie Mae and Freddie Mac, secondary mortgage lenders operating under United States government license, to encourage primary lender reliance on credit scoring systems; the purpose is to inject greater reliance on objective criteria into the lending process); *see also id.* (quoting Aida Alvarez, director of Federal Housing enterprise, recognizing that greater reliance on objective analysis protects against lending evils such as discrimination and disparate treatment, since credit scoring removes the human element of loan originators and underwriters from the process). *But see id.* (relating Alvarez' concerns about the negative long term implications of credit scoring); *id.* (relating that Dan McLaughlin, operations manager at Mortgage Electronics Registration Systems, expresses concerns that certain industry components might use artificially generated credit scores to identify and target potential lenders with average scores for denial).

Complying with statutory rules,[95] Brown requested and paid for a copy of his credit report.[96] By the time he figured out the credit denial was due to someone else's bad credit[97] and explained things to the lender, more than a month had passed.[98] The lender told Brown the loan could not be approved until and unless it received a corrected version of his credit report. Brown then embarked on the statutory journey necessary to correct his file.[99] First, he informed Infolink in writing of the error.[100] Infolink notified Brown in a form letter that he had to prove he was who he purported to be, and demonstrate that his file contained inaccuracies[101] before any changes would be made.[102] Brown complied while another month passed.[103] Infolink corrected Brown's file within the statutory time frame,[104] but still too late for him to save his bargain.

At trial, Brown sought to recover the £5000 difference between the cost of the house he originally sought to purchase, and what he would have to pay for a similar home.[105] Brown asserted he was never contacted regarding the troublesome credit report, claiming that notification would have allowed him to correct the information long before he applied for credit.[106] Infolink noted the lack of any statutory requirement compelling data management companies to verify information with data subjects.[107] It raised the statutory defense of reliance on data obtained from third parties,

---

95. DPA, *supra* note 6, part III, § 21(2) ("a data user shall not be obliged to supply any information . . . except in response to a request in writing and on payment of [a] fee. . .").

96. *Id.* (setting forth the statutory steps necessary for a data subject to obtain a copy of information kept by a data user).

97. In the hypothetical, the second Mr. Brown had lived in the same neighborhood as plaintiff, but moved some time previous to the events in question.

98. DPA, *supra* note 6, part III, § 21(6) (requiring that data users respond within 40 days of receipt of a request for file information).

99. *See* KNOW YOUR RIGHTS, *supra* note 4, at 8 (describing the steps necessary to correct credit report inaccuracies).

100. *Id.*

101. DPA, *supra* note 6, part III, § 21(4)(a).

102. *Id.* part III, § 24(1) (authorizing the court to rectify or erase data once proven to be inaccurate by plaintiff's efforts).

103. *See* KNOW YOUR RIGHTS, *supra* note 4, at 8 (relating procedures for correcting inaccuracies in personal data).

104. DPA, *supra* note 6, part III, § 21(6) (limiting how long data users have to respond to requests for information).

105. *Id.* part III, § 22(1) ("An individual who is the subject of personal data held by a data user and who suffers damage by reason of the inaccuracy. . . shall be entitled to compensation from the data user for that damage and for any distress which the individual has suffered by reason of the inaccuracy"). In this fact pattern, the home Brown originally wanted to purchase was discounted £5000 below market value as a result of foreclosure proceedings.

106. *See id.* part III, § 21(2) ("a data user shall not be obliged to supply any information . . . except in response to a request in writing and on payment of [a] fee. . ."). The Act does not require credit users to inform data subjects of their credit histories unless in response to an express request from the subject.

107. *See id.*

and claimed it exercised sufficient care[108] to insure the data was accurate at the material time.[109] Though he suffered substantial financial harm[110] Brown was denied recovery. However, despite the barriers to recovery, not all consumers experience the problems encountered by the hypothetical Mr. Brown as a result of inaccurate data,[111] and information technology can offer certain benefits to the modern consumer.[112]

C. *Some Benefits of Information Technology*

Information technology has revitalized contemporary marketing strategies.[113] Industries which recently ignored personal customer data are joining the global race to digitize and manage information.[114] The promise of increased revenues due to the expansion of traditional markets and the penetration of new, untapped ones spurs the growth of information businesses.[115] From a purely practical standpoint, only a spendthrift company invests today's dollars in shot-gun marketing[116] or relies on

---

108. *See id.* part III, § 22(3) ("In proceedings brought against any person by virtue of this section it shall be a defense to prove that he had taken such care as in all the circumstances was reasonably required to ensure the accuracy of the data at the material time"). In the hypothetical, Infolink's standard operating procedure was reasonable since it: a) regularly relied on data from the third parties in question; b) matched the neighborhood listed on Mr. Brown's application with that of the erroneous data subject; and c) had processed several other credit applications for the other Mr. Brown (all resulting in denials) within the past 90 days. For a real-life horror story, see *Regulation of Personal Data Flows*, *supra* note 12, at 62 (relating the debilitating experience of Mr. and Mrs. Michael Riley).

109. DPA, *supra* note 6, part III, § 22(3).

110. *See supra* notes 93-109 and accompanying text (relating Brown's loss of the opportunity to purchase a home for £5000 less than the house's actual market price).

111. *See* CREDIT SURVIVAL GUIDE, *supra* note 5, at 1 (noting erroneous information results in an outright denial of credit approximately 15% of applications, though up to 75% of all U.S. residents experience negative credit at some time).

112. *See infra* notes 131-41 and accompanying text (hypothesizing that consumers save time and money, and make more efficient purchasing decisions as a result of enhanced information technology).

113. *Flood Control*, *supra* note 64, at 479-80 (arguing that Internet access has created an unprecedented ability to compile and profit from the accumulation of personal data, leading to the ubiquitous acquisition of such information, and resulting in an accelerated erosion of a citizen's control over personal data). This emerging data base phenomenon will cause the costs of data storage to plummet, thereby increasing the appeal of data warehouse technology across a variety of platforms, ranging from commerce to law enforcement. *Id.*

114. *See infra* note 119; *see also Flood Control*, *supra* note 64, at 479 (noting that any person or entity with a computer, modem and access to the World Wide Web can record and track personal transactions of a sophisticated nature); *Privacy in the Information Economy*, *supra* note 76, at 198 (reporting the ability to trade information lists has grown into a three billion-dollar industry).

115. *Flood Control*, *supra* note 64, at 480 (describing the practical benefits of enhanced data management to consumer and industry).

116. *See* Keith V. Smith & Peter B. Murphy, *Market Planning for Small Business: Guidelines and Illustration*, <http://ce.ecn.purdue.edu./TAP/Publications/market-planning.html> (visited Jan. 21, 1997) (copy on file with *The Transnational Lawyer*) [hereinafter *Market Planning for Small Business*] (instructing business owners to avoid "shotgun" marketing strategies because they are overly broad, lacking in focus, and expensive in terms of time and resources). *See* Professor Philip Kotler, Address at the *Chartered Institute of Marketing* Annual Lecture (Oct. 7, 1996) (recommending companies shift marketing strategies from wasteful shotgun marketing to efficient customer-driven marketing). The article notes technology allows suppliers to develop an intimate relationship with a mass market and customize products to individual needs without charging a premium price. *Id.*

comparatively crude targeted marketing strategies[117] to attract or retain customers. Data compilation services can deliver the perfect prospect who is ready, willing and able to buy, at a fraction of traditional marketing costs.[118] An Internet entrepreneur can erect and publish a web page able to sift through over thirty million potential customers[119] for less than the cost of dinner for two at a fine restaurant.[120] Compare these meager start-up costs to those traditionally associated with launching a fledgling business[121] to understand the rapid growth of data management companies.[122] The personal computer has accomplished what diplomatic relations could not: a breakdown of national and international borders.[123]

---

117. *See Market Planning for Small Business*, *supra* note 116; *see also infra* notes 62-73 and accompanying text (discussing sophisticated, cross-platform marketing and information technology). To illustrate the difference between shotgun marketing strategies and sophisticated information-based marketing, consider two tactics. In one, a handful of pebbles is tossed into a crowd with hopes of hitting an unknown target who might be there. In the second, a sharpshooter equipped with telescopic sights is hired, given a color picture of the target, an itinerary of the target's daily activities, and positioned on the target's door-step. Throwing pebbles is shotgun marketing.

118. *See Browsing the Web*, *supra* note 18 (comparing costs of Internet marketing to traditional ways of generating prospective customers). Marketing expert David Scott Carlick suggests information technology can generate qualified prospects who respond to targeted advertising efforts for as little as US$3.00 each, a marketing investment that is "ridiculously low" compared to traditional methods. *Id.*

119. *See generally* Joe Clark, *The Online Universe: Find Out Why Some 30 Million People Count Themselves as Citizens of this Mysterious World*, TORONTO STAR, Oct. 20, 1994 (reporting the Internet has an estimated fifteen to twenty-five million users in ninety-two countries and is growing at the rate of five to eight percent per month); *see also* ARTHUR R. MILLER, THE ASSAULT ON PRIVACY 22 (1971) ("As if spread with a magic nutrient, information systems of every size, shape and form have sprouted and grown like weeds in recent years").

120. *See* Fischer, *supra* note 62 (reporting that an Internet Web page can be constructed and published for under US$50); *see id.* (quoting Charles Rubin, author of GUERILLA MARKETING ONLINE). In comments regarding the cost-effectiveness of Internet marketing, Rubin said, "Six months ago you could pay $1000 for Web programming. Now it's down to $20 a page." *Id. But see Browsing the Web*, *supra* note 118 (interviewing David Scott Carlick of Poppe Tyson, a graphic arts firm specializing in the design of Web pages). Aranoff notes that the complexity of pages demanded by large advertisers has driven Tyson's design costs up from an average of $20,000 to over $250,000 per assignment. *Id.*

121. *See SBA Financial Programs*, SBA Home Page, <http://www.sbaonline.sba.gov> (visited Feb. 19, 1997) (copy on file with *The Transnational Lawyer*) (noting the average size of an SBA-guaranteed loan is $175,000, and the average maturity is about eight years). The United States' Small Business Association guaranteed over 60,000 loans totaling $9.9 billion to small businesses in fiscal year 1995). *Id. See also How Much Money Do I Need to Get Started?*, SBA Home Page, <http://www.sbaonline.sba.gov> (visited Feb. 19, 1997) (copy on file with *The Transnational Lawyer*) (advising potential new business operators to have enough money on hand to cover operating expenses for at least a year).

122. *See* Jo-Ann Adams, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 COMPUTER & HIGH TECH. L.J. 403, 405 (1996) [hereinafter *Controlling Cyberspace*] (citing *Hearing on Internet Access: Subcomm. on Science of the House Committee on Science, Space and Technology*, 103d Cong., 2d Sess. 127 (1994) (statement of Jim Williams, Executive Director, FARNET Inc.)); *id.* (noting exponential decrease in cost of data delivery, from ten dollars per megabyte in 1987 to thirteen cents per megabyte in 1993, as a primary factor in attracting new users).

123. *See Restrictions on Data Flows*, *supra* note 24, at 471 (discussing the ways European Member states erected barriers restricting transfers of personal data across national borders in response to information technology). Conversely, the DPA has acted as a barrier to personal data transfer. *Id. See also Privacy Obstacle Course*, *supra* note 24, at 162 (relating the first inhibition on international data flow was imposed by the United Kingdom's Data Protection Registrar, under DPA authority). This 1990 prohibition barred the transfer of a mailing list from the United Kingdom to the United States. *Id.*

While enhanced proficiencies in targeting potential buyers means a potential windfall to savvy marketers,[124] the flaw in this economic picture is the same as the benefit: anyone with a few thousand dollars and a phone line can tap into huge stores of personal information.[125] With fortitude and at modest expense, one can even access highly sensitive information.[126] The rapid growth of technology exposes private individuals to greater risk of infringement because the rapid growth of information technology bypasses the traditional government approach to developing controls typically associated with the monitoring of business activities.[127] Whatever the law, when the technology that leads to the infringement has no practical restrictions on its use,[128] privacy interests are not respected. But privacy issues aside, consumers can benefit from commercial data management.[129]

So far, this Comment has addressed some of the ways data gatherers infringe privacy by harvesting, storing and disseminating immense blocks of personal data for commercial purposes.[130] Yet practical benefits[131] accrue to consumers given the

---

124. *See generally Controlling Cyberspace, supra* note 122 (suggesting new technology represents a windfall because corporate marketing expenditures can yield greater results due to more efficient targeting of prospective buyers, amplifying traditional returns on marketing expenditures).

125. *See supra* notes 119-20 and accompanying text (reporting the ease with which entrepreneurs can establish a presence on the Internet).

126. *See* Jeffrey Rothfeder, *What Happened to Privacy?* CHI. DLY. L. BULL. Apr. 13, 1993, at 6 (relating anecdotes about how easily the author obtained highly private information). For example, by paying an information company a small fee for computer access to its database, Rothfeder procured former U.S. Vice-President Dan Quayles' credit report, CBS New Anchor Dan Rather's recent credit transactions, and television personality Vanna White's home phone number. *Id.* The author has recent personal experience with this. While conducting a marketing survey for a company interested in establishing a credit-related business in Northern California, I established a computer link to a secondary provider of consumer credit reports. A nominal fee enabled me to acquire individual credit reports from all three major reporting bureaus within five minutes of relaying the request; just a name and social security number were required, though information could be located through residence history. The provider asked only that the company I represented assert a legitimate need for the reports. In this case, the company's need was legitimate: it obtained reports on behalf of data subjects who signed a release and request for the information, though one wonders whether illicit users of such information would hesitate to claim legitimacy.

127. *See Flood Control, supra* note 64, at 490 (questioning whether data protection laws are effective in providing protection of personal information privacy given the number of small databases subject to regulation). Data protection laws are likely to work best when the data collectors are few. *Id.* Bigger databases are easier to regulate because the data itself is more concentrated. *Id.* The growing number of small, continually updated databases frustrates legislative efforts to control information. *Id.* The international nature of data flows further limits the ability of any single nation to provide an adequate level of data protection. *Id.*

128. *See infra* notes 299-320 and accompanying text (outlining barriers to recovery faced by private individuals harmed by inaccurate personal data under the DPA).

129. *See infra* notes 131-41 and accompanying text (describing the positive benefits enjoyed by private consumers as a result of information technology).

130. *See Flood Control, supra* note 64, at 480-81 (suggesting that despite the benefits of large scale data management, consumers are without true recourse when they are harmed).

131. *See Flood Control, supra* note 64, at 480-81 (emphasizing consumer benefits such as reduced transaction and product costs, increased marketing efficiency and heightened customer satisfaction).

proper administration of data records.[132] Imagine a world where a consumer's personal buying patterns dictate the buying opportunities presented to him. Technology allows advertisers to identify products the prospect desires, without wasting valuable resources trying to sell something which is not wanted.[133] This means increased marketing efficiency and lower costs to the end user in a competitive, free market economy.[134]

Lending decisions may also be favorably influenced.[135] Reliance on computer-scoring protocols[136] to determine credit-worthiness eliminates the human bias which still plagues minorities seeking credit.[137] Objective credit scoring does not distinguish individuals on the basis of immutable characteristics[138] or according to social or ethnic variations.[139] Instead, objective measures of fiscal performance and responsibility evaluate loan applicants.[140] Over time, standardized scoring[141] can ameliorate the effects of bias on lending decisions.

---

132. *See id.* at 481 (pointing out a typical consumer convenience: local pizza delivery services now link caller ID systems to computer databases, allowing callers to be greeted by name and insuring accuracy of street names); *see also id.* at 488 (relating examples of how information technology can improve things for consumers). Restaurants build databases to handle customer orders; insurance companies identify whether clients eat fatty diets; and direct mail advertisers distribute the perfect junk mail which features only advertisements likely to be of interest to the recipient. *Id.*

133. *See id.* at 481-82 (characterizing this as"consumer friendly" data management which benefits citizens by increased quality of life).

134. *See supra* notes 131, 142 and accompanying text (analyzing the reduced expenses, lowered consumer costs and increased profits for businesses engaged in more efficient marketing activities).

135. *See infra* notes 138, 142-43 and accompanying text (describing the faster turn-around, lower cost, and greater objectivity associated with credit-scored loan applications).

136. *See id.*

137. *See Equal Owners - Nottingham Council Aiming to Change Attitudes of Mortgage Industry*, MORTGAGE FIN. GAZETTE, Dec. 1, 1992, *available in* LEXIS, Reuter Textline (highlighting racially based housing discrimination under Britain's Race Relations Act, in the cities of Rochdale and Leeds). For a broad overview of racial discrimination by United States mortgage lenders, see generally *Policy Statement*, *supra* note 83 (defining discriminatory lending as disparate treatment of otherwise similarly situated minorities and whites); Cathy Cloud & George Galston, *What Do We Know About Racial Discrimination in Mortgage Markets?*, 22 REV. BLACK POL. ECON. 101 (1993) (revealing overt discriminatory conduct on the part of loan officers dealing with black applicants ranging from a lack of interest to providing false or misleading information); *see generally The Color of Money: Home Mortgage Lending Practices Discriminate Against Blacks*, ATLANTA J. & CONST., May 14, 1988 (reporting pervasive discrimination by mortgage lenders in Atlanta, Georgia); Zina Gefter Greene, *Reviewing Loan Files for Evidence of Discrimination*, 28 J. MARSHALL L. REV. 351 (1995) (detailing the specific ways in which mortgage lenders discriminate in all phases of the lending process).

138. *See* Janet Sonntag, *The Debate Over Credit Scoring*, MORTGAGE BANKING, Nov. 1, 1995, at *1-2, *available in* 1995 WL 12414811 (reporting the secondary mortgage lender's preference for credit scoring as a more objective, reliable predictor of risk). The article quotes Ken Sacknoff, Director of Corporate Risk for GMAC Residential Funding Corporation, who praises credit scoring as free from the kind of subjectivity possible in traditional judgmental underwriting. *Id.* According to Sacknoff, computerized credit scoring is preferred over human operators because the process, "doesn't react to how you feel that day." *Id* at *2.

139. *See id.*

140. *See infra* note 143 and accompanying text (characterizing computer credit scoring as based on objective data, not racial or social differences).

141. *See supra* note 138 and *infra* notes 142-43 and accompanying text (describing the benefits of computerized credit-scoring).

The proper application of data warehouse technology offers British entrepreneurs an opportunity to open new markets and revive traditional ones by capitalizing on under-utilized markets primed for precise targeting and penetration.[142] This is tonic for a business community struggling to recover from years of mounting consumer debt, reduced spending and a relatively static population.[143] Really, the question is not whether commercial interests benefit from all this marvelous technology,[144] but whether it is being properly applied to protect individual privacy interests. Current data would suggest it is not.[145]

D. *Inadequate Protection of Privacy Interests*

The lack of CPA enforcement activity is one reason to suspect privacy interests are not adequately protected.[146] The personal database of virtually every British

---

142. *Cf. Is British Business Equipped for Recession?*, MGMT. ACCT., Apr. 5, 1991, at *1, *available in* LEXIS, Reuter Textline (reporting record levels of small business failures and a general increase in commercial bad debt). Dr. Brian Bailey, managing director of Infolink, one of the nation's largest data gatherers, predicted a business recovery for those companies relying on information technology. Bailey noted the importance of effective credit control and said, "Detailed information about the financial status of a prospect can be invaluable" in avoiding bad business dealings. *Id.*

143. *See, e.g., Controlling the Never Never With "Credipak 2000" from CCN*, ACCT., Dec. 7, 1988, at *1, *available in* LEXIS, Reuter Textline [hereinafter *Controlling the Never Never*] (discussing consumer's increased reliance on credit for purchasing power); *Responsible Lenders Spend Too Much Time and Effort in Processing Loan Applications*, MORTGAGE FIN. GAZETTE, Aug. 22, 1990, *available in* LEXIS, Reuter Textline (relating technological advances in managing personal information data based to improvements in lending efficiency, and reporting a rise in consumer debt to £43,000,000,000); Anthea Wynn, *Banking Services - Business Loans - Minimizing Risk and Default*, MORTGAGE FIN. GAZETTE, Apr. 5, 1991, *available in* LEXIS, Reuter Textline (reporting increased reliance of lenders on data warehouses to facilitate consumer loans. Evaluations by "live" personnel is considered cost prohibitive due to the relatively low dollar amounts involved); *Infolink Decision Services Launches Portrait - The First Ever Geo-Lifestyle Consumer Targeting System*, INFOLINK DECISION SERVICES LTD. PRESS RELEASE, Sept. 28, 1994, at *1, *available in* LEXIS, Reuter Textline [hereinafter *Portrait*] (announcing launch of PORTRAIT, an advanced data management and target marketing program capable of integrating lifestyle information and preferences into warehoused personal data); *CEO Interview - Dan McGlaughin of Equifax - Building Credit Globally*, INSTITUTIONAL INVESTOR, Apr. 29, 1996, *available in* LEXIS, Reuter Textline [hereinafter *CEO Interview*] (CEO of corporation which owns Infolink, the largest provider of consumer data in the UK, discusses the cooperation offered by banks and lending institutions in providing data on customers to enhance data base construction); *All Trade Deals*, *supra* note 63 (reporting a 250% increase in the number of business entities exporting data from one country to another in just 12 months, from 1987 to 88).

144. *See supra* notes 131-42 and accompanying text (relating the myriad ways in which information technology advances the cause of marketing efforts).

145. *See infra* note 150 (reporting poor compliance with DPA provisions compelling British data management companies to register as traders in personal data).

146. *See id.* (noting poor compliance by British companies with data registration requirements); *see also 12th Annual Report*, Data Protection Registrar Home Page, http://www.open.gov.uk/dpr/dprhome.htm (visited Feb. 19,1997) (copy on file with *The Transnational Lawyer*) [hereinafter Registrar Home Page] (surveying unregistered data management company awareness of DPA provisions). Only 51% of small (less than sixty employees) and 77% of large establishments were aware of the need to register. *Id.* Similarly, small companies were not aware of individuals' rights; only 36% had some familiarity, and fewer respondents from both large and small establishments were aware of individuals' rights than in the 1995 survey. *Id.* Public awareness of the Data Protection Act and Registration was even lower. *Id.* Just over one in ten respondents were spontaneously aware of the Act, cor-

citizen is managed to some extent by electronic processing.[147] Yet, the Office of Data Registrar[148] cannot report a single plaintiff victory against any one of the 250,000 companies regulated by the DPA in the twelve years since the Act's passage.[149] That record represents either admirable enforcement efforts resulting in strict compliance with all regulations by British business[150] or a lack of consumer efforts to pursue statutory redress.[151] Determining which is the more likely scenario requires examination of the relevant interests.

III. THE INCONSISTENT INTERESTS OF DATA GATHERERS, DATA USERS, AND DATA SUBJECTS

Achieving a proper balance between legitimate commercial interests and cherished personal liberties poses a conundrum[152] due to the intertwined, yet para-

---

responding to a general decline in understanding of the Act over the years. *Id.* Twenty-five percent of those aware of the Act knew it had something to do with protecting people's rights to personal information, but only 14% could name specific rights. *Id.*

147. *See, e.g., Controlling the Never Never, supra* note 143, at *1 (reporting on CCN's accumulation of 130 million separate records as part of personal databases on basically every household and adult person in the United Kingdom). CCN is a large database managers providing credit references and credit scoring services to lenders throughout Britain and the United Kingdom. *Id. See also Hard Line on Data Privacy, supra* note 63, at *1 (revealing that RBS Advanta, a VISA credit card provider, mailed two million solicitations at one time to British natives). The mailing list was gleaned from personal databases, despite DPA barriers to accessing such information. *Id.*

148. *See* Registrar Home Page, *supra* note 146 (describing the Data Registrar as an independent officer appointed by the Queen, and responsible for monitoring and enforcing compliance with the DPA). The Data Protection Registrar and a staff of one hundred is based in Wilmslow, Cheshire. *Id. See id* at Section Six (noting the Registrar can take enforcement action against a data user who has breached one or more of the eight Data Protection principles). *See also id.* (recounting that 2950 total complaints relating to the DPA were received in 1996). Of these, only 39 data users or .013% were actually charged, all with some offense related to registration requirements. *Id.* Of those charged, 39 were prosecuted for a failure to register or holding data for a purpose other than the one specified on the registration application, under DPA Section 5(1) or 5(2). *Id.* The remaining four were charged with violating the requirements of DPA, sched. 4, sec. 12(b) relating to the Registrar's unrestricted rights of entry and inspection of any registered company. *Id.* A total of £15,570 in fines were assessed against the offenders, for an average of £623 per offense; not one data user was prosecuted for misuse of data or data inaccuracy. *Id.*

149. *See* Registrar Home Page, *supra* note 146 (reporting the premiere case under the DPA to reach the House of Lords since its passage over a decade ago was heard in 1996). R. v. Brown (H.L.) 1996, found for defendant by holding that browsing of data by employees of a data user does not constitute a use of data under the law. *Id.*

150. This is an unlikely possibility. *See Lots of Companies Haven't Registered*, FIN. TIMES, Aug. 20, 1993 (reporting that just over half of all UK businesses required by the DPA to register as data users have done so).

151. *See id.* (discussing the latter alternative is probable; the low percentage of businesses registered as data users under the Act render the concept of *strict* adherence an oxymoron); *see also* Registrar Home Page, *supra* note 148 (noting that of nearly 3000 complaints against data users investigated by the Data Registrar in 1996, not one resulted in a prosecution for data misuse or inaccuracy).

152. *See* WEBSTER'S NEW ENCYCLOPEDIC DICTIONARY OF THE ENGLISH LANGUAGE 187 (1971) (defining conundrum as, "a sort of riddle in which some odd resemblance is proposed for discovery between things quite unlike").

doxical[153] interests of data gatherers, data users and data subjects. As foundation for addressing these interests, the first part of this section explains the barriers to maintaining file accuracy. Next examined are the conflicting interests of each group as they pertain to commercial lending transactions. The section concludes by discussing common interests.

A. *Reasons for Inaccurate Data*

As used in this Comment,[154] data gatherers are clearinghouses[155] for personal information about individuals. These entities harvest and then disseminate personal data to virtually any business engaged in credit transactions.[156] The data includes information about financial status and personal attributes[157] and lenders use it to determine creditworthiness.[158] This information is stockpiled in individual databases referred to as credit files,[159] which exist on virtually every individual who participates in financial transactions.[160] Each file contains biographical, employment, credit history, and public information.[161]

Typically, data gatherers do not determine this information through independent investigation of the data subject; credit grantors supply most of the information.[162] But advances in technology have rendered this type of data rather pedestrian for data gatherers like Infolink. This mega-provider[163] of information services now markets a new software program called Portrait.[164] Besides accessing information from traditional sources, Portrait searches Electoral Registers, County Court judgments, credit

---

153. *See infra* notes 299-320 and accompanying text (contrasting an individual consumer's responsibility for detecting and correcting personal database inaccuracies with statutory defenses absolving data gatherers of liability on a mere showing they have accumulated data in a reasonable fashion).

154. *See supra* note 1 (defining the term data gatherer as interchangeable with the terms data user, computer bureau and data warehouse).

155. RASOR, *supra* note 2, at 17 (characterizing credit reporting agencies as clearinghouses).

156. *Id.* at 18.

157. *Id.*

158. *See supra* note 1 (defining creditworthiness).

159. RAZOR, *supra* note 2, at 17.

160. *Id.*

161. *Id.* at 17-18 (noting personal data collected includes biographical information such as an individual's full name, aliases, address, identifying government number, and spouse's name; employment information like position, income, spouse's income, and place and duration of current and former employment; credit history showing all existing lines of credit, payment history by account, account balances, due dates, etc.; public information referencing arrest and conviction records, bankruptcies, judgments, liens, mortgages, marriage and divorce, and lawsuits).

162. *Id.* at 18 (identifying credit grantors as the data gatherer's main source of information).

163. *See generally CEO Interview*, *supra* note 143 (stating that acquiring United Kingdom-based Infolink pushed Equifax into dominating 45% of the market for credit information services market).

164. *See Portrait*, *supra* note 143, at *1 (characterizing the Portrait software system as the first consumer targeting system able to access and combine lifestyle and statistical information across United Kingdom borders). The software can predict specific consumer behavior for every post code neighborhood in England, Scotland, Wales and Northern Ireland. *Id.* at *2.

search activity, and employment statistics.[165] The program also captures lifestyle information detailing outside sources of income, hobbies, and personal interests.[166] This sort of large-scale data compilation is problematic in terms of maintaining data accuracy.[167] Thus, the more sources of information and the more complex the manipulation of that information, the greater the opportunity for inaccuracies.[168] Since data subjects do not have access to the database, it may be left to the data gatherer, the data provider, the end user, or all three to maintain file integrity.[169] An explanation of these competing interests follows.

B. *The Paradoxical Interests*

Data gatherers have strong incentives to amass personal data on a qualitative basis, and no serious government controls exist to compel its accuracy.[170] Data subjects theoretically have equally strong privacy interests in maintaining the integrity of personal information.[171] Reconciling these disparate concerns may depend on some affirmative shift in the balance of power between these competing interests.[172]

1. *The Interests of Data Gatherers*

Companies which stockpile and disseminate personal data derive revenue in a contradictory fashion, given their statutory duty for maintaining accurate records.[173] Typically, data warehouses receive fees[174] for receiving and disseminating private

---

165. *Id.* at *2.

166. *See id.* (explaining Portrait's initial database includes eleven million consumer survey responses to detailed lifestyle-sensitive questionnaires). Portrait combines survey responses and financial data from all other sources to reflect unique, evolving consumer behavior as part of a predictive database ideal for both financial and non-financial based businesses. *Id.*

167. *See* RASOR, *supra* note 2, at 19 (concluding it is beyond the ability of data gatherers harvesting information from hundreds of sources on millions of individuals to properly match the information collected to the data subject as accurately as smaller operations).

168. *See id.*

169. *See infra* notes 334-55 and accompanying text (proposing a mechanism to share the burden of file accuracy between interested parties).

170. *See infra* note 306 and accompanying text (describing the statutory test of reasonableness to determine if a data user has exercised sufficient care in ascertaining the accuracy of information).

171. *See supra* notes 47-48 and accompanying text (noting the grounding of privacy interests in traditional British concerns of personal liberty).

172. *See infra* notes 344-50 and accompanying text (proposing a shift in responsibility for maintaining accuracy in personal databases from data subjects, who are generally without ready access to the protected information, to data reporters, the root source of personal data).

173. *See supra* note 102 and accompanying text (defining a data user's statutory duty to maintain accurate information). *See generally infra* notes 246-66 and accompanying text (analyzing principal elements of the DPA).

174. CREDIT SURVIVAL GUIDE, *supra* note 5, at 4-5 (relating credit bureaus make money selling information to subscribers like banks, lenders, and potential employers, charging third parties for submitting personal data, and collecting fees from data subjects who wish to obtain a copy of their personal credit report).

data from and to third parties and the data subjects themselves.[175] Gross revenues are a direct function of the quantity of information acquired and disseminated.[176] The DPA allows data gatherers to obtain personal information from third parties without independent verification of the data's accuracy.[177] Further, maintaining accurate data bases does not reward data gatherers[178] who must expend additional resources to verify correctness.[179] Equivocally, though data gatherers retain fundamental control over the information to be protected,[180] the onus for detecting inaccuracies is on private individuals who do not enjoy the same ready access to the data as the data gatherer.[181] Moreover, it is not likely that data gatherers will be sued.[182] Plaintiffs harmed by inaccurate personal data must undergo both administrative[183] and judicial[184] review to obtain a judgment, and statutory defenses available to data gatherers act to preclude successful recovery.[185]

Given the dearth of consumer actions[186] and the relatively inconsequential penalties, one can understand why data providers may be tempted to overlook statu-

---

175. *See id.*

176. *See id.* (the more information gathered and disseminated by data managers, the more gross revenues generated); *see also* ANNUAL REPORT 1995, *supra* note 1 (reporting Fair, Isaac earnings in excess of US $113,000,000 as a provider of credit reports).

177. *See* DPA, *supra* note 6, part II, §§ 22-24 (absolving data users from liability so long as reasonable care was taken to insure the accuracy of third-party information). Reasonable care has not yet been defined by case law or statute.

178. *Cf.* GRIFFIN, *supra* note 5, at 168 (asserting credit bureaus gather information through blatant invasions of privacy, interpret it according to inequitable averaging formulas, and sell it to any party who can pay). Data gatherers make money by providing information which is presumed accurate. *Id.*

179. *See infra* notes 307-13 and accompanying text (describing the minimal effort required to achieve reasonableness in a determination of data accuracy). Any steps required beyond this bare minimum necessarily entails expenditures of time, money and employee resources beyond those currently expended. *See also* CREDIT SURVIVAL GUIDE, *supra* note 5, at 1 (declaring data gatherers do not have either time or inclination to check every individual consumer's credit report for accuracy).

180. *See supra* notes 155-62 and accompanying text (describing how data gatherers acquire and disseminate personal data).

181. *See infra* note 233 and accompanying text (defining the statutory steps a private individual must take to identify and correct inaccuracies). Individuals wishing to examine personal information held must pay a fee and make a written request. *Id.* Obtaining the report may take up to forty days. *Id. Cf. supra* note 126 (relating how data users can obtain personal information about virtually any individual within seconds of entering a request by computer).

182. *See supra* note 148 and accompanying text (reporting that every offense charged by the Data Registrar in 1996 involved a failure to register claim). Though the Registrar received nearly 3000 consumer complaints related to personal data usage, not one data user was charged with an offense. *Id.*

183. *See infra* note 233 and accompanying text (outlining the lengthy administrative review process required of individuals alleging inaccuracies in their personal data). The review period may take up to six months.

184. *See generally* DPA, *supra* note 6, part III, § 22(1) (specifying that individuals harmed due to inaccurate data may recover compensation for the damages and for any distress suffered as a result of the inaccuracy). The statute also details the statutory defense of reasonableness which allows data users to escape liability. *Id.* at § 22(3).

185. *See infra* notes 299-320 and accompanying text (reviewing statutory defenses).

186. *See supra* note 148 and accompanying text (specifying that no data users have been prosecuted under the DPA since its inception).

tory regulations.[187] Data gatherers want to preserve the rewards associated with the status quo.[188] Commercial interests may outweigh any inclination the industry might have to self-police[189] threats to privacy interests. This seems to be the case; nearly half the British companies[190] trading in personal data have forestalled government attempts to safeguard private data by ignoring regulations requiring them to register for periodic monitoring of business operations.[191] Thus, while data gatherers serve as the primary repositories of personal data, the DPA does not compel them to be accurate. Further, the Data Registrar fails to adequately monitor nearly half of the data management companies under its authority.

2. *The Interests of Lenders or Data Users*

Commercial lenders use personal data to determine the degree of risk associated with making a particular loan.[192] Inaccurate risk analysis results in decreased revenues[193] due to higher default rates, and ultimately, to escalating consumer costs.[194]

---

187. *Registrar Warns Companies About Data Protection Problems*, Office of the Data Protection Registrar, July 20, 1995 [hereinafter *Registrar Warns Companies*] (quoting Data Protection Registrar Elizabeth France). In response to poor industry compliance with statutory requirements, Ms. France commented, "... I am disappointed that more than 10 years after the introduction of this legislation so few organizations are fully aware of their responsibilities." *Id. See* DPA, *supra* note 6, part II, § 4(2)-(4) (enumerating the information a data user must supply to register under the DPA). Generally, a data user must specify: the nature of the business engaged in; the name and address of the data user; the type of personal data to be held and the purpose for which it is to be used; a description of the sources from which the data user will obtain information, and any entity to whom the user intends to disclose it; the name of any country outside the U.K. to which the user intends to transfer the data; and appropriate addresses for the receipt of requests from data subjects for access to the data. *Id.*

188. *See supra* notes 178-79 and accompanying text (regarding the increased expenses encountered by data gatherers to provide heightened verification of data accuracy). *But see* Denison Hatch, *Privacy: How Much Data Do We Really Need?*, TARGET MARKETING, Feb. 1, 1994, at *1, *available in* 1994 WL 13612733 [hereinafter *How Much Data*] (reporting marketing industry leader suggestions that data users either allow customers to selectively opt out of databases, or 'dumb down' operations to resist collecting minutiae about people's personal lives). Technology enables data gatherers to store, analyze, segment and use more data about more people than previously imaginable. *Id.* at *1. This same technology provides ever more ingenious ways to reach into the lives of data subjects. *Id.* But this may scare consumers. *Id.* at *4. A better approach would be for the industry to self-regulate its selection of what constitutes appropriate information. *Id.*

189. *See Flood Control*, *supra* note 64, at 400 (postulating the costs associated with curtailing data transfer might outweigh the benefits). *See generally How Much Data*, *supra* note 188, at *1 (reporting marketing industry opinions that information acquisition has reached the point of overkill).

190. *See Lots of Companies Haven't Registered*, *supra* note 150 (reporting just over half of all UK businesses required by law to register as data users under the DPA have done so).

191. *See id.*

192. *See infra* notes 193-99 and accompanying text (discussing how lenders use personal data in the form of credit reports or credit scores to evaluate loan risk).

193. *See Comptroller of Currency Finds Credit Flaws*, CREDIT RISK MGMT. REP., Nov. 20, 1995, *available in* 1995 WL 7500181 (cautioning lenders that lessening credit standards could increase loan defaults). Retail lenders expose their portfolios to increased risk by making it easier to qualify for credit. *Id. See also Sub-Prime Lenders Expand Market Presence: Competition Pressures Spur Credit Risk Concerns Relaxed Standards Threaten Profitability*, CREDIT RISK MGMT. REP., Dec. 30, 1996, *available in* 1996 WL 8309512 (reporting that loan recovery costs are increasing as marketplace competition forces lenders to offer funding to applicants with higher default

Lenders are in a difficult position: relaxed lending standards reduce investment returns due to inflated defaults,[195] but stricter standards mean fewer loans processed, resulting in an inefficient use of available capital.[196] To err excessively on either side has a negative ripple effect on interest rates.[197] When default rates rise due to relaxed lending standards, lenders must recoup their losses by raising interest rates.[198] As credit standards tighten, the number of loans granted falls, and interest rates again rise to maintain profits.[199] Under either scenario, private individuals pay more to obtain credit.

While apparent that inaccurate personal data leads to flawed lending decisions,[200] legitimate creditors traditionally exercise caution when making loans. A better-safe-than-sorry lending approach makes sense, especially since lenders do not have ready access to third-party sources of negative information about a particular applicant.[201] That is, lenders only have access to the actual credit report, not the data on which it is based.[202] Requiring lenders to verify the accuracy of reports is therefore impractical. While they would benefit from increased data accuracy, lenders cannot directly influence the correctness of personal information supplied by data gatherers.[203]

---

ratios). Some lenders are attracted to this segment of the borrowers because of large profit margins and low competition. *Id.* But servicing these loans demands lenders allocate additional resources to the monitoring and collection process. *Id. But see Lenders Can Profit From Sub-prime Auto Loans*, CREDIT RISK MGMT.. REP., July 1, 1996, *available in* 1996 WL 8309300 (distinguishing the high returns earned by lenders willing to finance high-risk borrowers with poor credit). Consumers with poor credit are willing to take out high interest rate loans to secure financing. *Id.* Lenders prepared to plan for the inevitable increased defaults can achieve high profitability. *Id.*

194. *See Lenders Can Profit From Sub-prime Auto Loans, supra* note 193 (explaining the increased interest rates charged to consumers as a result of increased lending risk).

195. *See* CONSUMER HANDBOOK, *supra* note 1 (specifying the effect of negative credit on loan repayment); *see also Credit Scoring Impact, supra* note 94, at 630-31 (reporting on U.S. regulatory agency efforts to encourage lender reliance on computer-scored credit evaluations, instead of those by human underwriters, as one way to decrease default rates).

196. Albert R. Karr, *Federal Drive to Curb Mortgage-Loan Bias Stirs Strong Backlash; Banks Say Regulators Meddle in Their Business; A Few Agencies Agree; The Hot Case of Chevy Chase*, WALL ST. J, Feb. 7, 1995 (discussing industry problems complying with regulations mandating liberalized lending practices).

197. *See supra* notes 193-95 and accompanying text (discussing how interest rates vary depending on lender risk).

198. *See id.* (discussing how interest rates vary depending on lender risk).

199. *See id.*

200. *See* CREDIT SURVIVAL GUIDE, *supra* note 5, at 1 (asserting 50% of all credit reports contain errors, and 15% of that information is negative enough to cause credit denial); *see also Regulation Personal Data Flows, supra* note 12, at 62 (reporting that 35% of consumers who pay to see their own credit reports find their information has been confused with someone else's).

201. *See supra* note 180 (noting data gatherers exercise primary control over personal information databases).

202. *See id.*; *see also* Sonntag, *supra* note 138, at *1 (questioning the impact of credit scoring on acceptance rates, compared to traditional evaluations of loan applicants). The credit scores yield a predictive ranking of how the candidate might perform instead of discrete information. *Id. See also* CREDIT SURVIVAL GUIDE, *supra* note 5, at 3 (revealing how a credit bureau report might indicate a loan applicant was thirty days late making a Visa credit card payment, but would be silent as to the specific payment record, dates of payment, possible reasons for the late-pay, or correspondence between the applicant and Visa).

203. *See supra* notes 202-03 (explaining how data users evaluate credit reports or scores, not gross personal data about a particular individual).

3. The Interests of Data Subjects

Data subjects, those most exposed to potential harm as the result of inaccurate date[204] are also least able to detect or ascertain inaccuracies.[205] An individual in this group is typically unaware of possible harm as a result of inaccurate data until after injury occurs,[206] and even then must seek remedy without voluntary cooperation from the very entities which profit by selling the disputed information.[207] Thus, the party in the worst position to protect important privacy interests has primary responsibility for doing so.

Given these conflicting interests, the conundrum is that individual rights may depend on information managers to elevate respect for individual privacy rights above pursuit of revenue and profitability.[208] The British government has apparently chosen to minimize its concern for personal liberties, as evidenced by its failure to register and monitor data users.[209] But other remedial choices are available: the government could either take a more aggressive approach to prosecuting and punishing commercial offenders,[210] or find a way to equitably balance private and commercial interests.[211]

C. The Intertwined Interests

Pricing strategies that reward data warehouses based on the quantity of information gathered[212] rather than for the accuracy of that information[213] harm both commercial and private interests. Lending decisions based on imprecise data are faulty, resulting in loss to the lender due to inefficient use of available capital, and to the

---

204. *See supra* notes 193-97 and accompanying text (reviewing the types of harm experienced by data subjects as a result of inaccurate personal data, ranging from higher loan origination fees, interest rates and requisite down payments to outright credit denial); *cf. supra* notes 181-89 and accompanying text (relating the relative ease with which data gatherers can escape liability for injury caused by inaccurate data, even when the consumer proves actual damages as a result of the error).

205. *See infra* note 233 (noting the lengths to which data subjects must go to determine what information about them is being held).

206. *See* GRIFFIN, *supra* note 5, at 155 (criticizing the fact that wronged borrowers typically find out about negative personal data after they are denied credit, not before).

207. *See infra* note 262 and accompanying text (detailing that data users are only obliged to provide information after receipt of a data subject's written request and fee).

208. *Cf. infra* notes 334-55 and accompanying text (suggesting alternate ways private and commercial interests might be balanced to protect personal data).

209. *See supra* note 148 and accompanying text (citing failure of Data Registrar's office to adequately enforce DPA provisions requiring registration of data users).

210. *See infra* notes 282-84 and accompanying text (criticizing the Data Registrar's failure to enforce the data protection principles relating to data accuracy).

211. *See infra* notes 334-55 and accompanying text (outlining proposals intended to heighten data protection by re-allocating responsibility for its accuracy).

212. *See supra* notes 174-75 and accompanying text (discussing the manner in which data gatherers generate revenue).

213. *See id.*

private individual who cannot gain credit.[214] Commercial interests suffer by reliance on data which may be inaccurate, resulting in denial of credit to an otherwise qualified candidate.[215] This increases costs to both lender and borrower.[216]

Conversely, inaccurate personal data harms private interests in two ways. First, error and therefore transgression usually occurs without the independent knowledge of the data subjects harmed.[217] Second, inaccurate data may result in the denial of credit which otherwise would have been granted.[218] The private citizen interested in securing credit ends up at the mercy[219] of a lender guided by credit scores,[220] not credit-worthiness.[221] Thus, it appears lenders and consumers share an interest in achieving the highest possible degree of file integrity. But the shared interests and the separate interests of data gatherers are at cross-purposes.[222]

Tension is predictable within the framework of a statutory scheme which protects privacy interests by relying on data gatherers,[223] the party with the most to lose and least to gain[224] to police data accuracy. Such a scheme is logically impaired, and

---

214. *See supra* notes 192-99 and accompanying text (examining increased risks to lenders and increased costs to consumers as a result of tightened credit standards and higher loan default rates).

215. *See* FACTS AND FALLACIES, *supra* note 1, at 15 (analyzing as high risk a credit score with a single thirty-day late payment in the last twelve months); *cf. supra* note 81 (reporting that from 35 to 50% of the negative information in a personal database is inaccurate). Applying these figures, an otherwise qualified loan applicant would thus be incorrectly rejected as high-risk up to half the time.

216. *See supra* notes 192-99 and accompanying text (reviewing the increases in loan fees, interest rates and loan recovery costs due to poor credit scores or reports).

217. *See supra* note 206 and accompanying text (relating that individuals typically discover detrimental information after credit is denied).

218. *See generally supra* note 215 and accompanying text (describing how a loan application may be rejected for a single late payment).

219. *See* DPA, *supra* note 6, part III, § 21(2) (requiring individuals denied credit to request a copy of their credit report in writing and pursue lengthy administrative review to compel its correction).

220. *See supra* notes 138-39, 142-43 and accompanying text (denoting increasing reliance by lenders on third-party evaluations of prospective loan candidates).

221. Not all commentators believe credit scoring based on traditional criteria reflects true creditworthiness for all applicants. *See Persistent Problem, supra* note 1, at 836 (suggesting that certain other criteria, such as successful utility and rent payments should be used as indicators of creditworthiness). *See generally Closing the Gap: A Guide to Equal Opportunity Lending*, FED. RESERVE BANK BOSTON 13 (1993) (urging lenders to consider utility, rent, telephone, insurance and medical bill payments when determining willingness to pay debts).

222. *See supra* notes 174-75 and accompanying text (emphasizing how revenue accrues to data gatherers based on the quantity of information received, processed and distributed). These businesses are not directly rewarded for maintaining file accuracy. *Id.*

223. *See infra* note 242 (compelling registration of data gatherers and data users under the DPA). Registration enables government monitoring of data gatherers. *See* DPA, *supra* note 6, part II, § 4(2) (granting the Data Registrar supervisory authority over data users and computer bureaus). Without registration, the government's ability to regulate the information industry is necessarily impaired. *Cf. supra* note 150 and accompanying text (noting just over half of the companies required by law to register have done so). One can surmise that a substantial portion of the data management industry apparently regards the registration requirement as irrelevant.

224. Data gatherers are not compelled to register, regardless of DPA requirements. *See supra* notes 148-51 and accompanying text (enumerating the minimal enforcement efforts undertaken by the DPA in 1996); *see also supra* note 187 (reporting the Data Registrar's frustration with the thousands of British companies yet to register as required); *supra* note 187 (concluding that data gatherers have chosen to disregard DPA registration requirements). Thus, any serious government attempts to compel registration would infringe to some extent on the degree

depends for success on one of two events. First, data gatherers and data users may voluntarily unite to protect the rights of data subjects,[225] conduct not required by law.[226] But expecting data gatherers to forego profits exceeds the boundaries of whatever devotion to privacy rights can reasonably be expected from businesses which make money by selling information.[227] The second event consists of a statutory solution that provides adequate and accessible protection to consumer rights, while sharing the burden of insuring data accuracy between all interested parties.[228] The next section evaluates Britain's attempt to provide such a solution.

IV. BRITAIN'S STATUTORY SOLUTION

Britain's Omnibus legislation regarding the use of personal information in a credit transaction[229] simplifies plaintiff's choice of law. If the violation involves an actual credit transaction, relief is available under the Consumer Credit Act (CCA).[230] Conversely, harm caused by the misuse of personal information subject to automatic manipulation falls under the Data Protection Act.[231] However, the comparative ease in determining an appropriate path to litigation has not enhanced the probability of recovery.[232] The statutory process is unwieldy and time-consuming,[233] and damages

---

of autonomy currently enjoyed by the data management industry; *cf. Privacy Obstacle Course*, *supra* note 24, at 156 (criticizing Britain's statutory filing requirements as unduly cumbersome). The Data Protection Registrar has acknowledged simplification of these procedures as an important goal. *Id.*

225. *See supra* note 188 and accompanying text (proposing that data gatherers should self-police to reduce the amount of extraneous data collected and to heighten file integrity); *cf. Banking Practice: Self-Regulation Versus Legislation*, EUROMONEY INT'L. FIN. LAW, Oct. 17, 1989, *available in* LEXIS, Reuter Textline (suggesting the British banking industry attempt to self-regulate the care given electronic processing of customer information before confronted with government intervention).

226. *See infra* note 257 and accompanying text (defining the statutory requirements regarding file accuracy).

227. *See supra* notes 174-75 and accompanying text (explaining how data gatherers process and sell information).

228. *See infra* notes 299-320 and accompanying text (outlining the barriers to recovery of damages for harm caused by inaccurate personal data).

229. The United Kingdom and Great Britain have consolidated consumer credit within two broad statutes. *See generally* CCA, *supra* note 50; DPA, *supra* note 6.

230. CCA, *supra* note 50.

231. DPA, *supra* note 6.

232. *See supra* note 148 and accompanying text (reporting enforcement statistics for 1996; out of nearly 3000 consumer complaints, no charges were brought against any registered data management company for a DPA violation relating to data accuracy). *Compare*, for example, United States laws regulating the use of personal data, including the Fair Credit Billing Act of 1974, 15 U.S.C. § 1666 (1988) (limiting maximum liability to creditor who fails to comply with reporting standards to $50); *with* Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681-1681t (1988) (providing for consumer recovery equal to amount of harm sustained only on proof of willful noncompliance by data vendor). *See also* Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681(n) (1988) (suggesting actions brought under this statute may be prolonged, with difficult-to-prove damages limited to the true financial harm sustained. Recovery under some statutes requires proof of willful negligence.

233. *See generally* Know Your Rights, *supra* note 99, at 2 (detailing the steps a consumer takes to compel correction of inaccurate personal data). This government-issued handbook breaks down the timeline for each step in the process as follows: Within 28 days of being turned down for credit, the person denied must request in writing the name and address of all credit reference agencies that the lender relied on for information. *Id.* at 6. The lender

are virtually inaccessible.[234] Thus, little incentive exists to bring an action. The following discussion is limited to the DPA given this Comment's narrow focus on personal data and privacy rights. The following section discusses the Act itself and concludes with an interpretation of its practical application.

A. *The Data Protection Act (DPA)*

The DPA advances eight principles[235] intended to safeguard personal information. The principles are realized through five related sections[236] expressed in forty-three separate statutes.[237] In addition, the Act establishes a Data Registrar[238] and Data Protection Tribunal[239] to register and monitor commercial data users and gatherers,[240] considered together in this section only as data holders.[241] Under the Act, all data holders must enlist with the Data Registrar,[242] which can monitor registered companies.[243] A series of schedules[244] augmented by the statutes explains the governing principles of the Registrar and Tribunal.[245]

---

has five days from receipt of the request to respond. *Id.* The person denied then requests a copy of his report from the designated credit agencies. *Id.* at 7. The agency has seven days from the date it receives the request to respond. *Id.* If the person denied finds an error, the credit reporting agency has twenty-eight days from the date it is notified of the error to either correct it, or notify the person denied that no correction will be made. *Id.* at 12. If the agency does not respond within twenty-eight days, the person denied has an additional twenty-eight days to send a notice of correction. *Id.* at 13. A notice of correction is a statement of up to 200 words explaining the negative information. *Id.* at 13-14. The notice is included in the individual's file, and is available for review by other potential lenders. *Id.* at 14. The credit reporting agency then must advise the person denied whether the notice has been added to their file. *Id.* If it amends a file or adds a notice of correction, it must send the details to any lender who has requested information about that file in the past six months. *Id.* If the agency fails to respond within twenty-eight days, the person denied can request intervention by the Director General of Fair Trading. *Id.* at 15. The Director General generally responds to the request within fourteen days, and attempts to solve any dispute within two months by administrative review. *Id.* at 16. This means a person denied credit due to inaccurate information must initiate and sustain express, written communication with up to three different, unrelated parties, over a time span of up to six months (182 days). *Id.*

234. *See infra* note 304-06 and accompanying text (specifying that damages are limited in scope, and noting how easily data gatherers might escape liability by raising the statutory defense of reasonableness).

235. *See generally* DPA, *supra* note 6, sched. 1, part I, §§ 1-8.

236. *Id.* Arrangement of Sections.

237. *Id.*

238. *See id.* part I, § 3(1)-(6) (creating a Data Protection Registrar).

239. *See id.* (creating a Data Protection Tribunal).

240. *See id.* part II, § 4(1 -(8) (requiring the registration of data users and gatherers with the Data Registrar).

241. *See id.* (separately defining data gatherers and data users).

242. *See generally id.* part II, § 4 (mandating the registration of data holders).

243. *See id.*

244. *See id.* scheds. 1-3.

245. *See generally id.*

1. The Principles

The first two principles establish that personal data must be fairly and lawfully obtained, processed and held.[246] Data provided by a person or business authorized[247] or required[248] to supply it is fairly obtained. Information is not obtained fairly when its supplier was deceived as to the purpose for which the information would be used.[249] The lawful purposes for which data can be held must be inferred from the statutes,[250] but presumedly data can be lawfully held for any legitimate purpose[251] specified by the data holder.[252]

The third and fourth principles regulate the retention and dissemination of personal data.[253] Under the Act, data holders may only use or disclose personal data according to the purpose for which it was originally obtained.[254] That purpose must be declared by data holders as part of the mandated registration process.[255] Additionally, the use must bear some adequate and relevant relation to the specified purpose.[256]

The fifth principle commands that data be accurate and contemporary.[257] Data is inaccurate if it is incorrect or misleading as to any factual matter.[258] But when inaccurate data results in harm, a data holder may escape liability by showing it exercised the care reasonably required under the circumstances to insure the data's

246. *See id.* sched. 1, part I, §§ 1-2.

247. *See id.* sched. 1, part II, § 2(a) (authorizing the release of information by or under any express enactment to supply it).

248. *See id.* sched. 1, part II, § 2(b) (requiring the release of information under any enactment or instrument imposing an international obligation on the United Kingdom).

249. *See id.* sched. 1, part II, § 1 (considering the conditions under which information was obtained when determining fairness).

250. *Id.* sched. 1, part II, § 2.

251. *See generally id.*, part II § 4(3)(b) (requiring that data holders must specify the purpose for which data are to be held or used as part of the registration process). The text does not specify what constitutes a lawful purpose. *But see* Registrar Home Page, *supra* note 146, at 1 (relying on civil and criminal precedent to determine if a breach of lawfulness has occurred). The Registrar considers a data principle breached where information is obtained illegally or processed to effect a contravention of the law. *Id. Cf.* DPA, *supra* note 6, part I, § 1(3)-(7) (implying that supplying information to lenders for the purpose of making credit decisions is a lawful purpose).

252. *See* DPA, *supra* note 6, part I, § 5(1)-(2)(a)-(d) (restricting the holding or distribution of data for any reason or to any party not specified by the data user or gatherer with respect to that data). The statute also prohibits the transfer of data to any country outside the United Kingdom other than one named by the entry. *Id.* part I, § 5(2)(e).

253. *Id.* sched. 1, part II, §§ 2-3.

254. *See id.* sched. 1, part II, § 2 (requiring that data holders specify the purpose for which data will be used when registering with the Data Registrar); *see also* Registrar Home Page, *supra* note 146 (identifying the declaration of purpose as a simple process). The Registrar allows registrants to register purpose within broad categories of intended disclosure, such as to licensed credit reference agencies, or to lenders. *Id.*

255. DPA, *supra* note 6, sched. 1, part II, § 2.

256. *Id.* sched. 1, part I, § 4 (specifying the use to which data is put cannot be excessive in relation to the purpose designated by the data holder upon registration).

257. *Id.* sched. 1, part I, § 5.

258. *Id.* part III, § 22(4).

accuracy.[259] The Act does not define the standard of care necessary to satisfy the "reasonably required" test.[260] As the final provision regulating data held by a third party, principle six prohibits data holders from retaining information any longer than necessary to satisfy the holder's specified purpose.[261]

Under the seventh principle, interested individuals are allowed to find out whether information about them is held, and the details of that information.[262] While this principle also provides for correction or erasure of information,[263] it simultaneously notes that such alterations will only occur under certain circumstances.[264] Also, companies that process and distribute information to third-party data users must erect security measures against unauthorized access to or distribution of personal data.[265] However, the Act does not delineate what constitutes adequate security measures.[266]

2. *The Data Registrar and Tribunal*

Though appointed by the Queen,[267] the Data Registrar is an independent officer who reports directly to Parliament.[268] The Registrar's duties include maintaining a public register of data holders, disseminating information about the Act, reviewing consumer complaints about data misuse, and promoting compliance with the Act through public relations efforts and by prosecuting those in violation of the Act's registration conditions.[269] Since the Registrar can only monitor the activities of pro-

---

259. *See id.* part III, § 22(3) (providing data holders with a complete defense so long as reasonable care was taken to insure accuracy at the material time).

260. *See generally id.*

261. *Id.* sched. 1, part I, § 6. The statute does not set a ceiling on how long data might ultimately be held. *Id.*

262. *Id.* sched. 1, part I, § 7(a)(i)-(ii) (compelling the data holder to provide requested information at reasonable intervals, without unnecessary delay or expense). *See id.* sched. 1, part II, §5(2) (restricting the data subject's access to reasonable intervals to be determined by the nature of the data, purpose for which it is held, and the frequency it is altered); *but see id.* part III, § 21(2) (requiring data subjects to request such information in writing and pay the specified fee before any information is released).

263. *Id.* sched. 1, part I, § 7(b).

264. *Id.* sched. 1, part II, § 5(3); *cf. supra* notes 259-60 (outlining the defenses available to data holders when a private individual is harmed by inaccurate information).

265. DPA, *supra* note 6, sched. 1, part I, § 8 (denoting that computer bureaux must employ adequate security measures against unauthorized access to, or alteration, disclosure or destruction of personal data). The principle also requires protection against accidental loss or destruction. *Id.*

266. *See id.* sched. 1, part II, § 6(a)-(b) (explaining that evaluating security measures takes into account the nature of data held, the harm which might be caused by unauthorized access, and the specific security measures taken against loss). This analysis of circumstances intimates a case-by-case approach to determining the adequacy of security measures, rather than a bright-line rule. *See id.*

267. *See generally id.* part I, § 3(1)-(2) (authorizing and describing the statutory establishment of the Data Registrar).

268. *See* Registrar Home Page, *supra* note 146.

269. *See id.* (relating the duties and responsibilities of the Data Registrar).

perly matriculated entities,[270] it devotes much of its energies to determining whether companies have subscribed.[271] But despite the fact that only registered companies may lawfully trade in personal data, barely half of the data users compelled to sign up by the Act have actually done so.[272]

Violating registration requirements exposes data holders to possible criminal prosecution.[273] But, breaching the data protection principles regulating data accuracy is not a criminal offense.[274] This means private citizens must pursue civil recovery, since individuals are not directly affected by a violation of the registration principles.[275] Instead, data holders who obtain information unfairly or unlawfully, distribute the information for a purpose other than the one specified, or fail to maintain accurate information are subject merely to supervisory intervention by the Data Registrar.[276]

3. *A Practical Application of the Act*

The DPA looks good on paper. Ostensibly, it requires data holders to register for monitoring with an official government authority,[277] and provides for criminal prosecution of unregistered companies.[278] The Act compels data users to comply with certain standards in the gathering, processing and dissemination of personal data.[279] It even creates an independent body[280] to monitor the management of personal data with jurisdiction to intervene when data principles are violated.[281] But a lack of

---

270. *See generally* DPA, *supra* note 6, part II, § 6 (outlining the application process for companies registering as data holders under the Act). *Id.* part II, § 4 (specifying that applicants must include certain information necessary for monitoring purposes including the data holders name and address, the purposes to which data will be put, and the parties to whom it will be distributed).

271. *See* Registrar Home Page, *supra* note 146 (declaring the main objective of the Registrar is to identify data holders not yet registered, and compel their registration); *see also id.* Sanctions and Liabilities (noting the Registrar's general policy of prosecuting unregistered data users).

272. *See id.* at 1 (quoting the Data Registrar's frustration with failed registration attempts).

273. *See id.* Sanctions and Liabilities (describing the criminal offenses created under the Act, and expressed in the principles).

274. *See id.* (absenting breaches of the principles from criminal prosecution).

275. *See id.* Sanction and Liabilities (describing criminal offenses under the Act).

276. *See* DPA, *supra* note 6, part II, § 10(1)-(9) and accompanying text (defining the steps necessary for a private individual to institute formal proceedings against a data holder).

277. *See supra* note 240 (outlining registration requirements).

278. *See supra* note 273 (noting that failure to register may constitute a criminal offense).

279. *See generally supra* notes 246-66 and accompanying text (outlining the DPA's standards and requirements for handling personal data).

280. *See supra* note 267 (authorizing creation of a Data Registrar)..

281. *See supra* note 281 and accompanying text (describing the Data Registrar's enforcement authority).

enforcement authority,[282] an absence of bright-line rules,[283] and a failed effort to register data holders[284] cripples the Act.

The DPA forces harmed data subjects to endure both an extended administrative appeal[285] and civil litigation[286] to obtain relief. As discussed below, chances for recovery are minimal given the statutory defenses available to data holders.[287] Efforts to protect data privacy are also hampered by the fact that data holders can violate data protection principles without risk of criminal prosecution.[288] Literally hundreds of thousands of data holders[289] are not even subject to government monitoring of their data management practices, thanks to the Registrar's failed attempts to compel registration.[290]

The lack of clear language as to prohibited conduct creates another impediment to enforcement of privacy rights.[291] The Act is silent regarding purposes for which data can be used,[292] the standard of care necessary to insure data accuracy,[293] the length of time data can be held,[294] and the type of security measures required to protect data.[295] Presumably, courts must apply a case-by-case analysis, leaving each

282. *See generally supra* note 273 and accompanying text (granting the Registrar power to prosecute data holders for failing to register). Conversely, the statute categorizes breaches of data protection principles related to the accuracy of personal information as non-criminal offenses, subject only to administrative review. *See id.*

283. *See supra* notes 251, 261, 266 and accompanying text (regarding the lack of clear rules defining specific conduct prohibited by the DPA).

284. *See What Does the Act Cover?, supra* note 58 (bemoaning the Registrar's failure to register nearly half the companies dealing in personal data management).

285. *See supra* note 233 (outlining the up to six-month appeal process mandated by the DPA).

286. *See infra* notes 299-320 and accompanying text (describing the civil litigation process).

287. *See infra* notes 306-13 and accompanying text (asserting that statutory defenses available to data holders constitute barriers precluding recovery by most plaintiffs).

288. *See supra* note 274 and accompanying text (establishing that while failure to register may constitute a criminal offense under the DPA, breaches of the data protection principles relating to accuracy are not).

289. *See supra* note 187 (reporting that less than half of the country's data holders had registered by mid-1996).

290. *See id.*

291. *See The First Data Protection Principle*, Data Protection Home Page, <http://www.open.gov.uk/dpr/dprhome.htm> (visited Nov. 5, 1996) (copy on file with *The Transnational Lawyer)* [hereinafter *First Data Protection Principle*] (responding to complaints by data users regarding the DPA's lack of clarity in defining standards and requirements under the law). The Registrar asserts that appropriate guidance can only fairly be determined case-by-case in light of industry practices and consumer expectations. *Id.* The compliance and fair practice standards therefore respond to changes in these factors. *Id.* The Registrar does not articulate how private individuals should gauge the current standards, or how industry might predict future modifications in interpretation.

292. *But see supra* note 254 and accompanying text (articulating the Data Registrar's simplistic, categorical approach to specifying purpose).

293. *See supra* note 257 and accompanying text (requiring correctness without defining any accuracy standards under the DPA).

294. *See supra* note 261 and accompanying text (specifying the length of time data can be held under the DPA).

295. *See supra* note 265 and accompanying text (demanding but not defining adequate security measures).

alleged infraction open to interpretation.[296] In combination, these weaknesses in the Act allow data holders to act with impunity, favoring commercial interests over those of data subjects. The following examination of remedies advances this conclusion: under the DPA, harmed consumers are left with no realistic expectations of recovery.[297]

B. Current Remedies

The harmed consumer may recover damages under the DPA when a credit reference agency fails to disclose filed information to the data subject[298] or fails to correct inaccurate information.[299] The party bringing the action bears the burden[300] of developing a body of evidence which is greater than the proof opposing plaintiff's view.[301] The consumer must demonstrate real damages as a result of inaccurate information caused by the data user's failure to reasonably ensure accurate information.[302] Proving damages is a considerable hurdle; plaintiff must demonstrate the loss of some real economic benefit.[303] Even when per se relief is available,[304] damages are limited to £200, (roughly US$500) per violation.[305] In addition to limited damages, the DPA's statutory defenses also aid potential data offenders.[306]

---

296. *See supra* note 148 and accompanying text (reporting the absence of civil actions against data gatherers). A case-by-case approach is presumed since no bright-line rules exist to guide the court, and no cases law exists to suggest common law approaches. *Id. But see First Data Protection Principle, supra* note 291 (adopting a common law approach to determining whether data are processed lawfully). The Registrar interprets 'lawful processing' in light of court holdings in related areas of jurisprudence defining that which is unlawful. *Id.*

297. *See infra* notes 307-13 (examining how available statutory remedies serve the interests of data holders by frustrating consumer chances of recovery).

298. *See* DPA, *supra* note 6, part III, § 21(1).

299. *See id.* part III, § 22 (1).

300. 17 HALSBURY'S LAWS OF ENGLAND, para. 13 (4th ed. 1979) (establishing which party bears the burden of proof in this type of civil litigation).

301. *Id.* (commentary explains this burden is somewhat greater than a preponderance of the evidence standard, and something less than a beyond a reasonable doubt standard).

302. *See infra* note 307 and accompanying text (defining the statutory test of reasonableness data users must attain to verify the accuracy of data obtained from third parties).

303. *See supra* notes 91-110 and accompanying text (relating the hypothetical experiences of Mr. Brown). The fictional Brown sought £5000 as compensation for the economic harm he suffered as a result of inaccurate credit data. But without some further proof that Brown was actually deprived of the benefit of a bargain, the award sought resembles unjust enrichment more than equitable recovery. Black's Law Dictionary defines the benefit of the bargain as a rule under which a defrauded purchaser may recover the difference between the real and the represented value of the property purchased. BLACK'S LAW DICTIONARY 158 (6th ed. 1990). The unjust enrichment doctrine is an alternate path to recovery, defined as the general principle that one party should not be permitted unjustly to enrich himself at the expense of another. *Id* at 1535.

304. *See* CCA, *supra* note 50, part X, § 158 (limiting statutory damages according to a fixed schedule).

305. *Id.*

306. *See* DPA, *supra* note 6, part III, § 22(2)-(3) (recognizing that compensation for damages due to inaccuracies won't be awarded when the challenged information is obtained from a third party, so long as the data user took such care as was reasonably required to ensure the data's accuracy at the material time); CCA, *supra* note 50, sched. 1, § 159(6) (defining the statutory penalty for failure to correct inaccurate data as a Level 4 violation, which carries a maximum fine of £1000). Neither authority levies any fine for incorrect data if the data user simply

The Data Protection Act requires only that a data warehouse exercise reasonable care in the compilation of personal information.[307] Reasonable care is not defined by case law,[308] but the data user satisfies the statutory test by a mere showing that it regularly relies on the third party that provided the erroneous information, and exerted some effort to match the data provided to the right data subject.[309] This is a meager burden for the typical data gatherer to bear, since the statutory requirements essentially mirror the day-to-day business of building personal data bases.[310] A data gatherer necessarily relies on data from third parties to amass personal information; outside data is the sole source for the creation of individual credit histories.[311] Once received, some minimal effort is necessary to match incoming information with a particular personal file.[312] This means the data gatherer complies with the DPA just by operating in a conscientious manner.[313] Unfortunately, compliance with this standard does not equate with file accuracy.[314] Thus, even though a private citizen can seek relief through a single government agency the remedies available are simply not worth the trouble.[315]

Chances of recovery are slim, and there is no guarantee the successful plaintiff will ever be granted the credit originally sought.[316] In fact, a record of the legal conflict may become a permanent part of the litigant's personal credit history, alerting all future data and end users that this individual represents a possible irritant to busi-

---

corrects the file prior to government intervention, regardless of any harm caused to the consumer.

307. *See id.*

308. *See supra* note 148 and accompanying text (reporting that to date the Data Registrar has not prosecuted a single case relating to misuse or inaccuracy of data).

309. *See supra* note 306.

310. *See supra* notes 63-73, 118-24, 133-44 and accompanying text (describing how data gatherers accumulate, process and distribute information).

311. *See* CREDIT SURVIVAL GUIDE, *supra* note 5, at 3-4 (detailing specific third-party sources from which data gatherers derive information). None of the sources listed includes information independently generated by the data gatherer. *But see id.* at 2 (noting that investigative consumer reports, sometimes used by mortgage lenders, depend on information developed through the direct efforts of the lender or its agent). Investigative reports may include personal interviews with the loan applicant's friends, neighbors, landlord and employer. *Id.*

312. *See* DPA, *supra* note 6, part III, § 22(2)-(3) (negating liability to the data user so long as it took reasonable care to ensure the data's accuracy at the material time). The statute does not define reasonable care.

313. *See supra* notes 310-12 and accompanying text (reviewing the manner in which data gatherers accumulate information, the third-party sources relied on, and the statutory defenses available).

314. *See supra* notes 75-76, 81-82, 167 and accompanying text (relating the high percentage of data errors traditionally associated with companies that gather and distribute personal data).

315. *See supra* note 233 and accompanying text (defining the statutory steps consumers seeking recovery must take); *supra* note 302 and accompanying text (requiring consumers allegedly harmed when a data gatherer breaches a data protection principle to prove actual damages). Proving actual damages depends on subjective interpretations of the effects of improper data management. Plaintiff must prove both that she suffered actual damages and the amount of those damages. This is difficult given the subjective nature of credit decisions. *See* FACTS AND FALLACIES, *supra* note 1, at 4-9 (describing the number of independent subjective factors evaluated in credit decisions). It might be difficult to prove plaintiff would have qualified for credit even if the error had not occurred, given the subjective nature of the information. *Id.*

316. *See* FACTS AND FALLACIES, *supra* note 1, at 4-9. Presumedly a successful plaintiff would still be required to re-apply for credit subject to evaluation by the prospective lender.

ness as usual.[317] Finally, plaintiff may find it difficult to support the underlying cause of action when no bright-line rule exists to constrain the data gatherer,[318] who can escape liability by proving the steps it took to verify data accuracy were reasonable.[319]

For example, in the normal course of business operations, a lender (or end user) relies on the computer bureau, data warehouse or credit reference agency to transmit the personal data file of the applicant for credit.[320] While theoretically possible for each data user to build and maintain its own file about every prospective loan candidate, economies of scale forbid such a practice.[321] The additional financial burden assumed by the end user/credit provider forced to generate personal data would reflect back on the consumers as increases in loan generation fees, interest rates, and cost of goods.[322] In a free-market economy, absent statutory authority compelling in-house verification, companies choosing to self-verify would be at a competitive disadvantage compared to those relying on outside vendors.[323] Thus, an approach requiring end users to verify the accuracy of personal data creates burdens of commercial impracticality difficult to overcome at the present time.[324] A better alternative would require both providers and gatherers of personal data to follow modified procedures designed to insure the greatest practicable degree of accuracy for each

317. *See* CREDIT SURVIVAL GUIDE, *supra* note 5, at 4 (describing lawsuits as a matter of public record subject to gathering and inclusion in personal data files).

318. *See supra* notes 291-96 and accompanying text (criticizing the lack of clearly defined statutory provisions).

319. *See supra* note 306 (explaining the statutory defense of reasonableness).

320. *See* CREDIT SURVIVAL GUIDE, *supra* note 5, at 1 (noting credit bureaus "are supposed to provide the correct and current information which creditors want and need to make informed business decisions").

321. A data user wishing to build and maintain an independent database of all potential loan applicants faces a considerable challenge. They would have to replicate a database already managed by commercial data gatherers. *See supra* notes 143, 164 and accompanying text (noting that companies like Infolink and CCN are repositories for credit-related information on virtually every household in the United Kingdom). This would necessitate establishing links to a vast array of third-party sources which already report information to data gatherers on a reciprocal basis. *See supra* note 161 and accompanying text (noting third party sources of personal data). Without access to a data gatherer, the lender must necessarily bear the entire cost of replicating this data, and could not spread the cost among a vast network of other users. *See* Registrar Home Page, *supra* note 146 (reporting that approximately 250,000 British companies currently trade in personal data). Inevitably, the lender's cost of obtaining background information would increase. This places the lender at a competitive disadvantage: loan costs would increase, but the lender couldn't recoup them in a market where other lenders could still obtain personal data for a nominal fee from outside sources. Finally, lenders who generate information independently would assume the statutory duty to register and operate as data gatherers, accompanied by the obligation to verify information accuracy, thus exposing them to liability. *See* DPA, *supra* note 6, part II, § 4(2) (requiring registration of data users and computer bureaus); *id.* part III, § 22(1) (entitling individuals damaged by inaccurate personal data to compensation).

322. *See supra* notes 131-41 and accompanying text (discussing the ways consumers benefit from enhanced marketing efficiency).

323. *See supra* note 322.

324. *See id.*

individual file.[325] Four methods to achieving greater accuracy are proposed in the following section.

V. FOUR PROPOSALS TO HEIGHTEN PROTECTION OF PRIVACY INTERESTS

Trading in personal data is a multi-billion dollar business, with virtually unlimited potential to change the shape of product marketing, sales and revenue.[326] Soon, any business that does not exploit personal information databases will suffer, and more aggressive competitors will gain market share.[327] Conceivably, this might be what motivates those engaged in the commercial use of personal data to resist government attempts at regulation.[328] This creates a suspicion that industry self-regulation will ultimately fail to adequately safeguard personal interests in data protection[329] absent some shift in statutory duties to protect those interests.[330] In response, this section considers a number of ways to preserve the threatened interests.

One way to achieve a proper balance between personal privacy and commercial interests is to shift the burden of maintaining file accuracy from the consumer, with limited access to relevant data,[331] to the data provider and data gatherer, the primary managers of the information.[332] Redefining the reasonable steps data gatherers must take to verify data accuracy according to a bright-line standard would provide additional protection. Additionally, adopting a per se approach to damages likely increases a harmed individual's chances of recovery. Finally, providing a mechanism for data subjects to opt out of inclusion in commercial databases represents the ultimate protection of privacy interests.

325. *See infra* notes 334-75 and accompanying text (discussing proposed solutions to the current conflict between privacy interests, and the business goals of data gatherers).

326. *See supra* notes 131-42 and accompanying text (describing the impact of information technology and Internet access on marketing strategies, practices and costs).

327. *See Flood Control, supra* note 64, at 479 (theorizing the Internet represents a "mother lode of consumer profile information"). Froomkin asserts data collection will continue to grow in five areas (medical history, government records, personal movements, transactions, and reading and viewing habits) to cover most of modern life. *Id.* at 483.

328. *See supra* note 150 (emphasizing barely half of the companies required to register under the DPA have done so).

329. It is apparent that DPA enforcement to date has focused largely on registration violations. *See supra* note 148 and accompanying text (presenting Data Registrar enforcement statistics). Of 2,950 consumer complaints in 1996, no charges relating to inaccurate data were successfully prosecuted. The only offenses prosecuted were for breach of registration requirements. *Id.*; *see also supra* note 224 (noting the Data Registrar's admission that administrative processing and review procedures should be simplified).

330. *See infra* notes 334-55 and accompanying text (advocating a shifting of the burden between data gatherers and users to safeguard personal data accuracy).

331. *See supra* note 233 and accompanying text (denoting the steps consumers must go through to obtain a copy of their credit reports).

332. *See supra* notes 63-73, 118-24, 133-44 and accompanying text (examining the process by which personal data is gathered).

A. *Shifting the Burden: Notification and Verification*

A greater degree of exactness is within the practical reach of data gatherers. The same technology that maximizes the large-scale accumulation of data lends itself to a verification process that would enhance file accuracy.[333] Companies that stockpile personal data should periodically notify[334] private individuals of the information contained in their data file. Most data discrepancies arise as the result of error[335] and may not be detected until the consumer is denied credit. The amount of inaccurate information received and processed could be reduced by mailing consumers a simplified data report with an invitation to notify the data warehouse of inaccuracies.[336]

The first step in any verification procedure recognizes that data gatherers harvest, package and offer information for sale to end users.[337] Yet the subject of that information is typically excluded from the process associated with building a file.[338] Verification aims at increasing file accuracy; inviting input from the individual with the greatest ability to recognize a potential error could streamline the process.[339] The following steps outline a simple verification process designed to identify gross potential errors and to expressly notify individuals that negative personal information exists.[340]

---

333. Theoretically, the same software, hardware and personnel that receive, process and post incoming information, and prepare, package and transmit outgoing information can fulfill the type of verification function envisioned in this Comment.

334. *See* CREDIT SURVIVAL GUIDE, *supra* note 5, at 4-5 (describing how data gatherers generate revenue by acquiring, transmitting and otherwise exercising control over personal data); *cf. supra* note 262 accompanying text (noting statutory requirements that data subjects pay to find out what information is held about them).

335. *See* CREDIT SURVIVAL GUIDE, *supra* note 5, at 1 (maintaining that nearly half of all credit reports contain errors, nearly 15% of which are serious enough to result in outright denial of credit); *see also Regulation of Personal Data Flows*, *supra* note 12, at 62 (reporting that information belonging to one person is wrongly attributed to someone else 35% of the time).

336. *See Regulation of Personal Data Flows*, *supra* note 12, at 77 (expressing the belief that consumers should be given the right to opt out of inclusion in certain mailing list databases). British data gatherers are already required to allow data subjects to be excluded from data processing when information about them is collected for one purpose, then sold to a marketing company for some other use. *See id.* at 71 (emphasizing how the European Directive compels member states including the United Kingdom and thereby Great Britain to grant such a right). Therefore, data gatherers necessarily have systems in place to communicate with data subjects. *Id.* Requiring periodic notification presents a minimal burden, the cost of which would undoubtedly be passed along to commercial customers. *Id.*

337. *See supra* notes 62-73, 174-75 and accompanying text (describing the manner in which personal information is gathered and marketed).

338. *See* CREDIT SURVIVAL GUIDE, *supra* note 5, at 3 (listing the sources which data gatherers rely on to construct a personal database; the individual data subject is not on the list). *But see supra* note 233 and accompanying text (explaining that data holders must include a statement written by the data subject to explain a legitimate negative item if one is provided).

339. Theoretically, an individual's personal knowledge and insight about confidential information is not yet commercially available.

340. *See supra* notes 334, 351-53 and accompanying text (theorizing a notification process would not work an undue hardship on data gatherers); *see also supra* notes 334-55 and accompanying text (outlining the notification and verification process proposed in this Comment).

A positive or neutral report[341] would be regarded as presumptively correct.[342] This protects private individuals, who are not harmed by positive or neutral information.

Second, a third-party reporting a negative item[343] would be required to expressly verify the correctness of the information. This verification would become a permanent part of the individual's record.[344] However, a negative item would be justified only when the reporting third-party maintains sufficient general ledger evidence to support the allegation of accuracy.[345] Failure or refusal to verify would preclude the data gatherer from recognizing or posting the negative information.

Once verified, the negative information would be placed in a hold status lasting for sixty days.[346] The data gatherer assumes the duty of making reasonable efforts[347] to contact the private individual concerned during that sixty day period, and advise her that a negative item has been reported, the name, address and phone number of the reporting entity, and the statutory recourse available.[348] The individual affected could either notify the data warehouse that the information is correct or fail to respond within sixty days, in which case the negative entry stands. Or, the individual could challenge the report.[349]

---

341. *See* CREDIT SURVIVAL GUIDE, *supra* note 5, at 20 (identifying a positive or good credit account as one where required payments are made on time). Account types are classified from positive to negative in the following descending order: Positive credit rating by oldest to most current date; accounts showing one or more 30-day late payment; accounts with one or more sixty-day late payments; those with 90-day late payments; 120 days late payments; paid collection accounts; unpaid collection accounts; paid judgments; unpaid judgments, paid to unpaid tax liens; foreclosures, repossessions, evictions, notices of default, delinquent school loans, and unpaid child support. *Id.* at 20-21.

342. The presumption of accuracy could be overcome by a satisfactory showing of account deficiency by the data gatherer or user.

343. For example, consumer accounts charged-off as uncollectible bad debt, late payments on a contractual obligation, or repossession of consumer goods being purchased on installment would be regarded as negative information. *See supra* note 342 and accompanying text (ranking credit accounts from positive to negative).

344. For example, the verification might be accomplished by using a form indicating the reporting party has substantiated the negative information by reviewing pertinent documents, and asserting the data is true and correct. *Cf. supra* note 6 and accompanying text (noting the DPA's silence regarding ways to insure data accuracy).

345. General ledger information might include a copy of the contract or agreement binding the customer to the obligation, a copy of the general ledger where payments were posted, including the date of receipt and entry, and name of the individual who made the entries; and a copy of any correspondence between the customer and the lender, including dates of receipt and mailing.

346. *See* DPA, *supra* note 6, part III, § 21(6) (granting a data gatherer 40 days to respond to a consumer's request that inaccurate data be corrected). The proposed period adds 20 days to notify the data subject.

347. *See supra* note 334 and accompanying text (describing the relatively slight additional burden this would impose on the data gatherer). Conceivably, notification would benefit data gatherers, who would receive updated, marketable information regarding data subjects.

348. *See generally supra* note 99 and accompanying text (describing the contents of a government booklet which explains the statutory steps necessary to correct incorrect personal data). This information could be replicated in a two-sided, single page flyer, and enclosed with the notification mailing.

349. *See supra* note 233 and accompanying text (detailing the steps necessary to correct erroneous personal data). The affected individual would simply comply with statutory guidelines.

Data gatherers may protest against the additional resources required by any heightened verification process.[350] But the proposed approach shares the extra burdens involved in improving file accuracy between third-party reporters of information and data gatherers.[351] Plus, shifting much of the burden for accuracy to the reporting parties should reduce the amount of incorrect data submitted.[352] This affirmative approach to maintaining data integrity serves legitimate commercial interests which benefit as a result of accurate information,[353] and individual privacy rights which benefit by greater protection from inaccurate information.[354]

B. Modify the Statutory Defense of Reasonableness

The DPA allows a data user to escape liability for inaccurate file information so long as it takes reasonable steps to insure the accuracy of information provided to it by the data subject or a third party.[355] The statute does not define what is reasonable and the dearth of case law[356] on the subject leaves the concept ill-defined. Under the heightened scrutiny of a verification process like that outlined above,[357] *reasonable* may be defined by a bright-line rule: a reasonable effort occurs where the data user complies with the verification process dictated by statute. Before submitting derogatory information the reporting party must verify its accuracy by reviewing appropriate supporting documents.[358] Under this scheme, posting negative infor-

---

350. *See supra* note 143 and accompanying text (detailing the amounts of data handled by British data gatherers); *see also supra* note 337 and accompanying text (comparing the notification burden to the statutory burden involved in granting consumers the right to opt out of direct mailing lists).

351. *See supra* note 337 and accompanying text (explaining how the burden of insuring data accuracy may be shared more equally between data gatherers and data users).

352. *See supra* notes 75-76, 81-82, 167 and accompanying text (reporting the high percentages of inaccurate personal data reported by data gatherers). Conversely, any costs born by a commercial entity as a result of compliance with statutory requirements compelling accuracy are ultimately passed along to the consumer. It seems reasonable to require each loan applicant to pay a few shillings, dollars or Deutchmarks more to insure enhanced reliability and greater protection of personal privacy interests.

353. *See supra* notes 131-42 and accompanying text (regarding the increased profits enjoyed by businesses as the result of greater accuracy in personal data).

354. *See supra* note 148 and accompanying text (noting the Data Registrar's general lack of enforcement activity); *see also supra* notes 257-60 and accompanying text (focusing on the data protection principles devoted to insuring the accuracy of information held about private individuals).

355. DPA, *supra* note 6, part III, § 22(2) ("In proceedings brought against any person by virtue of this section it shall be a defense to prove that he had taken such care as in all the circumstances was reasonably required to ensure the accuracy of the data at the material time").

356. *See supra* note 91 (noting that no cases relating to data misuse have been successfully prosecuted under the DPA in the 12 years since its inception).

357. *See supra* notes 334-55 and accompanying text (proposing a verification process intended to increase file accuracy).

358. *See supra* note 346 (demanding the review of general ledger and relevant documents, not just computer print-outs of payment histories to support a negative entry).

mation without verification is presumptively unreasonable.[359] The advantages of this approach are two-fold.

First, statutory enforcement of the proposed verification process adds strength to any policy favoring increased accuracy in personal data.[360] As noted earlier, current statutes do not compel any of the entities involved in the reporting, accumulating, processing or distribution of personal data to insure a high degree of accuracy.[361] Second, under this plan data gatherers will not avoid liability by a mere showing of reasonableness in reliance on third-party information.[362] Instead, data users must meet the proposed bright-line test of reasonableness to avoid damages.[363]

C. A Per Se Approach to Damages

The greatest burden a consumer faces when harmed by inaccurate data is proving actual damages.[364] At best, this is a subjective analysis subject to rebuttal by the offending party.[365] A better solution is to adopt a per se approach to damages. Under this scheme, the plaintiff is entitled to statutory awards once proof of the wrong is established.[366] Since damages inevitably result from one type of financial transaction or another, awards might relate to the amount of harm suffered as a function of the type of transaction.[367]

Of course, individuals can only be harmed by inaccurate private data when subject to data gathering. Allowing private individuals to absent themselves from commercial databases is one way to prevent harm to privacy interests. The next section proposes just such an alternative.

D. Opting Out of the System

Both private citizens and lenders participate in the organized collection of personal data: citizens seek credit and lenders seek a reasonable return on credit granted.

---

359. Hypothetically, the presumption might be rebutted by a showing that but for an error by the reporting party or data gatherer, verification would have complied with the statute.

360. *See supra* notes 279-81 and accompanying text (reasoning the DPA is intended to safeguard the accuracy of personal data).

361. *See supra* note 307 and accompanying text (discussing the statutory defense of reasonableness available to data users).

362. *See id.* (regarding the reasonableness defense).

363. *Cf. id.* (defining the current statutory defense).

364. DPA, *supra* note 6, part II, §§ 22-24 (requiring proof of damages).

365. *See supra* notes 300-01 and accompanying text (relating the requisite standard of proof in civil litigation).

366. *Cf.* CCA, *supra* note 50, § 167 and sched. 1 (enumerating statutory damages awarded for violations). A similar strategy could be employed by the DPA.

367. For example, an individual wrongly denied a mortgage loan recovers the difference in costs between what they would have paid in loan costs and interest rates if the loan had been approved, and the present cost for the same loan. Damages may be adjusted to conform with pre-set ceilings. In the alternative, the lender could mitigate damages by providing a loan at the same rates and terms as the one denied.

Given this, both parties should comprehend that informed credit decisions depend to some extent on proper risk analysis.[368] Parity[369] exists when both parties gain from the exchange. Here, credit is granted to the applicant, and the lender earns interest. But some individuals have no interest in commerce, and may never want to buy a television, a car, a house or an airplane ticket on credit[370] Suppose these individuals have no desire to receive catalogs from retail outlets, business opportunities from real estate moguls, or subscription solicitations from magazine vendors.[371] Finally, suppose that certain individuals are not prospects for any conceivable marketing strategy or consumer purchase. Such individuals should be allowed to opt out of all data bases assembling, processing and distributing personal information for the purpose of commercial transactions.[372]

By opting out, the individual would assume responsibility for managing personal credit records. Most likely, a predisposition against individuals who opt out would exist in most lending environments.[373] But, data warehouses would not have to expend resources maintaining information on these individuals.[374] Parity exists because an entity in the business of selling information about individuals interested in participating in credit transactions is relieved of maintaining information about an individual with no interest in such a pursuit.

VI. CONCLUSION

Computer and information technology has evolved to the point where an ability to access personal data has enhanced value.[375] Protecting important privacy interests as represented by personal data has been subordinated to furthering commercial

---

368. *See supra* notes 138-39, 142-43 and accompanying text (discussing the effects of risk analysis on lending decisions).

369. BLACK'S LAW DICTIONARY 1115 (6th ed. 1990) (defining parity as equality in amount or value).

370. Not every person seeks credit. *See Hard Line on Data Privacy, supra* note 63, at *2 (reporting approximately 120,000 persons responded to a solicitation reaching two million persons). Individuals were prescreened and pre-selected to receive a Visa credit card. *Id.* Typically, only one to one and one-half percent of those solicited respond. *Id.*

371. *See supra* notes 62-73, 118-24, 133-44 and accompanying text (regarding the volume of direct marketing efforts based on information technology).

372. Some commentators have posited an ability to opt out might better serve privacy interests. *See Regulation of Personal Data Flows, supra* note 12, at 77 (suggesting data protection could be heightened by allowing consumers to opt out of direct marketing lists for a variety of reasons); *cf. How Much Data, supra* note 188, at *5 (noting that a number of direct marketers offer customers the chance to opt out). The opt out language is prominently featured in bold type at the top of marketing materials. From six to seven percent of the people contacted elect to be removed from the mailing list. *Id. But see* Deborah Hagan, *Credit Reporting and Privacy Issues*, 80 ILL. B.J. 412, 415 (asserting that trading off some personal privacy is a condition of living in a credit-based economy).

373. *See supra* notes 193-99 and accompanying text (discussing increasing lender reliance on electronically-processed personal data to make informed lending decisions).

374. Government databases may be the proper repository for biographical information including name, age, address, date of birth, military service, government identification number, and government health benefits.

375. *See supra* notes 63-73 and accompanying text (discussing the growth of information technology).

interests in perfecting informed lending decisions. As a result, personal privacy is in danger of infringement.[376] British legislative efforts to protect personal privacy, though well-intentioned, have not kept pace with this evolution and provide little recourse for harmed consumers.[377]

Data gatherers engaged in the harvesting, storage, and dissemination of private information are both the primary threat to personal privacy[378] and the chief beneficiary of failed government efforts to establish blanket consumer protection.[379] The personal data processed by these companies is often based on erroneous information provided by third-party reporters.[380] Erroneous data results in harm to consumers in the form of either denial of credit, or increased costs to borrow.[381] A data management problem endures because information harvesters are rewarded for quantity, rather than quality of information; no statutory incentive exists to compel affirmative verification of personal databases.[382]

The solution to this dilemma lies between the data warehouses themselves, as the ultimate managers of personal data, and the third parties who report personal data to the warehouses. A simple process requiring verification of negative and potentially erroneous information using existing software, systems, networks, protocols and personnel[383] would improve the accuracy of personal data. The procedures are not invasive, and spread the burden of verification between those who gather, store and distribute data, and those providing data in the first place. The procedures require the reporting entity to confirm negative information before posting to individual databases.[384] Adopting this proposal may lead to reduced errors, improved communication between third party reporters, data gatherers, and the consumer, reduced harm to important privacy interests, and increased marketing efficiency due to economies of scale.[385]

376. *See supra* notes 62-64 and accompanying text (examining how privacy interests are threatened by information technology).

377. *See supra* note 148 and accompanying text (noting the Data Registrar's lack of enforcement activity).

378. *See infra* note 380.

379. *See supra* notes 188-90 and accompanying text (examining how data gatherers benefit most by a maintenance of the status quo).

380. *See supra* notes 75-76, 81-82, 167 and accompanying text (reporting the high percentage of errors in data held for large-scale processing).

381. *See supra* notes 193-99, 214-15 and accompanying text (evaluating the increased costs borne by consumers as a result of imperfect lending decisions).

382. *See supra* notes 176-78, 299-320 and accompanying text (emphasizing that data gatherers are rewarded for processing quantities of information, and that statutory defenses make it difficult for harmed consumers to recover damages).

383. *See supra* notes 351-54 and accompanying text (relating how data gatherers and users could cooperate to accomplish greater accuracy in personal databases).

384. *See supra* notes 334-55 and accompanying text (proposing that data gatherers and third-party reporters of information share the burden of verifying the accuracy of information recounted).

385. *See supra* notes 334-37 and accompanying text (hypothesizing possible benefits of a system intended to heighten the accuracy of personal data).

Personal data could be further protected by requiring data users to advise data subjects of their file content through direct, periodic contact.[386] Further, damages which are difficult to prove under the current regulations should be presumed when a private individual suffers due to mismanagement of personal data.[387] Finally, any private individual should be allowed to affirmatively opt out of the scheme of personal data management.[388] The only data maintained on these individuals would be necessary biographical information.[389] This option creates the ultimate protection of personal data: a shield of anonymity against accidental, intentional or merely inevitable infringement of their personal right to privacy.

---

386. *See supra* notes 334-55 and accompanying text (suggesting ways to accomplish enhanced verification of potentially erroneous information).

387. *See supra* notes 367-68 and accompanying text (postulating such an approach would increase consumer chances for recovery).

388. *See supra* notes 373-75 and accompanying text (positing that both data gatherers and disinterested individuals benefit by such an option).

389. *See supra* note 375 (specifying examples of necessary biographical and social data).