Cornell International Law Journal

Volume 34
Issue 2 *2001*

Article 4

Legislating U.S. Data Privacy in the Context of National Identification Numbers: Models from South Africa and the United Kingdom

R. Brian Black

Legislating U.S. Data Privacy in the Context of National Identification Numbers: Models From South Africa and the United Kingdom

R. Brian Black*

* J.D., Cornell Law School, 2001; A.B., Harvard College, 1997. The author would like to thank Marvin Johnson for his insightful comments. black@post.harvard.edu.

34 CORNELL INT'L L.J. 397 (2001)

Introduction

In the United States, people use credit card numbers, bank account numbers, phone numbers, driver's license numbers, club membership numbers, student ID numbers, tax ID numbers . . . numbers ad infinitum.[1] Most citizens assume they know which entities use a specific identifier, usually under the expectation that only the issuing party utilizes any personal information provided in exchange for the benefits of the identifier. Unfortunately, with a single national identification number linking various sources of information, this assumption may no longer be correct.

The prevalent use of national identification numbers triggers an imminent privacy crisis regarding control of information. As technological advances make it easier to collate data, government agencies and corporate firms seek to collect personal information about people either from the individuals themselves or by sharing data with other organizations. National identification numbers facilitate the accumulation of information in unanticipated ways and, accordingly, serve as a focal point for this privacy crisis. These numbers epitomize the danger to privacy posed by the organizational hunger for efficient information techniques. As each day passes, organizations' databases grow, with a corresponding increase in the power inequity between organizations and individuals. Possessing a mere number reveals pages of personal information.

In the United States, many privacy advocates label the social security number a de facto national identification number.[2] Viewed historically, the current uses for social security numbers do not belie this label, especially in the context of increasingly invasive technological advances. As the technology emerged to misuse social security numbers, Congress enacted privacy protections against government use. Yet, as corporate use expanded, Congress eroded privacy laws by granting exemptions to government agencies and mandated that government and corporate entities

1. Many government or corporate groups issue cards identifying the bearer by name and corresponding number. Although the cards themselves raise concerns, this Note focuses on the numbers linking the card carrier to information maintained by the issuing government or corporation. *Cf.* Simon Davies, Privacy International, *Identity Cards: Frequently Asked Questions* (last modified Aug. 24, 1996), *at* http://www.privacy.org/pi/activities/idcard/idcard_faq.html ("Generally speaking, particularly in advanced societies, the key element of the card is its number.").

2. *E.g.*, Press Release, American Civil Liberties Union, *National ID Card Measure Comes Before Congress; ACLU Urges Committee to Stop Big Brother* (May 13, 1997), *available at* http://www.aclu.org/news/n051397a.html.

collect and use social security numbers. In the courts, protections against the abuse of social security numbers fared poorly due to some courts' failure to recognize the dangers posed by technological advances.

With data profiling and identity numbers threatening individuals worldwide, the European Union addressed these concerns by regulating use of personal information.[3] The United States government responded by negotiating safe harbor provisions for U.S. businesses with EU customers.[4] Due to the current lack of national privacy protection,[5] the U.S. government will likely continue to pursue a policy of exempting U.S. citizens from international privacy protections until significant national efforts increase citizens' control over personal information.[6] This policy, however, ignores

3. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Data Privacy Directive].

4. U.S. Dep't of Commerce, *Safe Harbor Privacy Principles* (July 21, 2000), *available at* http://www.export.gov/safeharbor/shprinciplesfinal.htm.

5. *See* Mayer Brown & Platt, *U.S., EU Reach "Safe Harbour" Agreement On Personal Data Transfers*, INT'L BRIEFING, Nov. 24, 2000, LEXIS, News Library, ALLNWS File (noting that unlike some countries, the United States needed the safe harbor provisions because "[t]here is no single national law or single point of national enforcement . . . . Privacy regulation in the United States . . . is sectoral in nature.").

6. E.g., Margret Johnston, *U.S. to Kick Off Series of "Safe Harbor" Briefings*, INFOWORLD DAILY NEWS, Jan. 4, 2001, LEXIS, News Library, INFDLY File (describing the Commerce Department's two-year struggle to negotiate the safe harbor provisions as "hard-fought" and noting current efforts to educate companies on the benefits of the provisions because only twelve businesses registered in the first month); *cf.* Stephen Lawson, *Former U.S. Trade Official: Privacy Headaches Will Linger*, COMPUTERWORLD, Mar. 27, 2001, *at* http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59023,00.html (discussing a former U.S. trade official's concerns about the dismal prospects for multinational companies trying to cope with the disparate national data-privacy approaches given her experiences assisting in the negotiations for the U.S.-EU safe harbor provisions). Despite the painstaking efforts to arrange the safe harbor provisions, Congress recently attacked EU efforts to implement the Data Privacy Directive. Patrick Ross, CNET News, *Congress Fears European Privacy Standards* (Mar. 8, 2001), *at* http://news.cnet.com/news/0-1005-202-5070401.html (expressing the commitment of some members of Congress to corporate self-regulation for data privacy and their dissatisfaction with the safe harbor provisions); *see also The EU Data Protection Directive: Implications for the U.S. Privacy Debate Before the House Subcomm. on Commerce, Trade, and Consumer Protection of the Comm. on Energy and Commerce*, 107th Cong. (2001). The Bush Administration also undermined the efficacy of the safe harbor provisions by criticizing the European Union's efforts to formulate "model contracts" for EU firms to use when dealing with U.S. firms. Press Release, Treasury Dep't, Treasury/Commerce Letter to European Commission on Model Contracts (Mar, 23, 2001), *available at* http://www.treas.gov/press/releases/po116.htm ("[T]here is a serious danger the adoption of the standard clauses as drafted will create a de facto standard that would raise the bar for U.S. and foreign firms . . . ."); Glenn R. Simpson, *U.S. Officials Criticize Rules on EU Privacy*, WALL ST. J., Mar. 27, 2001, 2001 WL-WSJ 2858294 (noting that a former negotiator for the Clinton Administration also considered the EU's efforts as a violation of the safe harbor agreement); *see also An Examination of Existing Federal Statutes Addressing Information Privacy Before the House Subcomm. on Commerce, Trade, and Consumer Protection of the Comm. on Energy and Commerce*, 107th Cong. (2001) (statement of Representative William Tauzin) ("I was pleased to see the new Administration's letter to our European colleagues questioning the so-called "model contracts". . . . [It] seems the model contracts are an effort to undercut the so-called "safe-harbor" and further impose a European privacy approach on the U.S.").

the larger international trend toward enacting national privacy legislation in response to the EU Directive and the increased public sentiment supporting personal privacy.[7]

Correcting the United States' counterproductive policy decisions on privacy will require a substantial and comprehensive solution. Given the multifaceted nature of privacy, it helps to limit the discussion to one issue that encompasses the problems with the U.S. privacy protections generally. Also, given the diverse approaches to privacy protection, models in other countries provide established examples from which to formulate a U.S. solution. Therefore, using national identification numbers as a focal point and based on foreign privacy models, this Note suggests broad modifications to U.S. privacy jurisprudence that will conform current protections to international standards while maintaining efficiency.[8]

Accordingly, this Note will consider the United Kingdom and South Africa's responses to national identification numbers as informative alternatives to the U.S. solution for personal privacy in the computer age.[9] These countries provide helpful comparative models because the United Kingdom represents a more traditional privacy regime while South Africa has embarked on a radical tack that incorporates technological components. Unlike the United States, the British government issues separate identification numbers for different agency services, and a single department has sole responsibility for individuals' privacy. Alternatively, South Africa recently decided to implement a national identification system predicated on the use of smart cards[10] that verify identity and personal infor-

7. *E.g.*, Brian Krebs, *US Businesses Slow to Adopt EU Safe Harbor Agreement*, NEWSBYTES, Jan. 4, 2001, LEXIS, News Library, NWSBYT File (noting that Argentina enacted privacy legislation more stringent than the EU Directive); William New, *Privacy Concerns, Regulations on the Rise in Japan*, NAT'L J. TECH. DAILY, Dec. 1, 2000, LEXIS, News Library, TCHDLY File (describing Japan's desire to negotiate a safe harbor provision in favor of national self-regulation, but noting that more than fifty percent of local governments already had privacy regulations and that privacy protections were a "politically popular" topic for national legislation); Patrick Thibodeau, *Europe's Privacy Laws May Become Global Standard*, COMPUTERWORLD, Mar. 12, 2001, at http://computerworld.com/cwi/story/0,1199,NAV47_STO58498,00.html (noting that "the issue for the U.S. is whether it can buck international trends on privacy"); Ruth Walker, *With Nod to Europe, Canada Tightens Data Privacy*, CHRISTIAN SCI. MONITOR, Jan. 10, 2001, at 11 (describing the influence of the EU's Directive on Canada's new privacy legislation and noting that Australia and India also passed legislation to conform with the Directive).

8. As evidenced by the tension between the European Union and United States over the Data Privacy Directive, *supra* notes 3-7 and accompanying text, any U.S. solution must ultimately be rooted in the U.S. political system and jurisprudence, not forced by compliance with a treaty or agreement to which the United States is not a party. Also, any solution derived from foreign privacy models must conform to U.S. values that may differ from the originating country. *See infra* Part III; *infra* notes 258, 364, 366.

9. To minimize issues of compatibility and possible U.S. resistance to extranational strategies, only countries with roughly similar roots in a common law heritage were initially considered. Differences between the political and judicial traditions of the United States and the United Kingdom and South Africa will be noted when relevant.

10. "Similar to a credit card, a smart card stores information on an integrated microprocessor chip located within it." Smart Card Forum, *What is a Smart Card?* (last visited Jan. 23, 2000), *at* http://www.smartcrd.com/info/whatis/whatis.htm.

mation using a central database. To improve information control, the United States must resolve the tension between organizational efficiency and individual privacy with the United Kingdom and South Africa's alternatives in mind.

Due to the minimal efficacy of existing protections, resolving the tension between efficiency and privacy requires a massive philosophical shift in U.S. law,[11] albeit a return to basic principles of freedom and liberty. The current U.S. structure for information control breaks down because the jurisprudence for informational privacy fails to recognize the importance of every bit of personal data. Legal rights should empower individuals as active members of society. If organizations make decisions for a person based on an individualized and invasive profiling, however, the individual loses autonomy. The U.S. must formulate a new structure for information control that restores individual autonomy and allows citizens to dictate how personal information will be used and disseminated, while aligning its policy with international privacy standards. To set the stage for this solution, Part I describes the technological potential for collection of personal information, traces the historical development of social security numbers, and explores the U.S. legal response to violations of informational privacy.

Part II sketches brief characterizations of the United Kingdom and South Africa national identification approaches by categorizing both models according to three aspects: information management—how the country compiles and disseminates information; privacy enforcement—how the country ensures compliance with existing privacy protections; and citizens' access to information—how the country provides an individual access to information regarding that person.[12] These characterizations supply the raw material to establish a U.S. structure for information control.

Part III introduces the concept of structural modification and the structural factors for evaluation. Finally, Part IV examines the effectiveness of alternatives using the United Kingdom and South Africa's methods to address privacy concerns and concludes that a decentralized database network with centralized privacy protections and centralized access for individuals to personal information resolves many privacy concerns while maintaining reasonable government and corporate functionality. Also, Part

11. The failure of U.S. jurisprudence to recognize the importance and precarious position of information privacy has motivated other commentators to advocate a change in the privacy paradigm. Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy (Oct. 17, 2000) (unpublished manuscript, on file with author) (using Franz Kafka's *The Trial* as the literary groundwork for an alternative paradigm to the framework for privacy concerns based on George Orwell's "Big Brother").

12. While these aspects also apply to the United States, background on the U.S. approach to national identification numbers is provided historically to emphasize the critical need for a new approach implicated by the steady decline in privacy protections. In formulating a new structure for information control, the U.S. jurisprudence is recharacterized according to these aspects. *Infra* Part IV.A-C.

IV evaluates the structure's potential operation and impact in the United States.

I. National Identification Numbers in the United States

The most basic tension spurring the privacy crisis involves the conflict between efficiency and privacy. The administrative efficiency associated with numbers encourages government agencies and private firms to adopt national identification numbers.[13] References to efficient administration by number, however, invoke images of a totalitarian state, such as Jews branded by Nazi Germany or prison inmates referred to only by number.[14] Identity reduced to a number eases cross-referencing among databases, simplifies the verification process, and increases government's flexibility.[15] Yet, identification numbers consolidate information to create an instant

13. Bowen v. Roy, 476 U.S. 693, 710-11 (1986) (acknowledging the use of social security numbers to match database records as the "Federal Government's most cost-effective tool for verification or investigation in the prevention and detection of fraud, waste and abuse" (quoting THE PRESIDENT'S PRIVATE SECTOR SURVEY ON COST CONTROL, MANAGEMENT OFFICE SELECTED ISSUES—INFORMATION GAP IN THE FEDERAL GOVERNMENT 90 (1984))); Green v. Philbrook, 576 F.2d 440, 445 (2d Cir. 1978); S. REP. NO. 93-1356 (1974), *reprinted in* 1974 U.S.C.C.A.N. 8133, 8152; *see* GENERAL ACCOUNTING OFFICE, SOCIAL SECURITY: GOVERNMENT AND COMMERCIAL USE OF THE SOCIAL SECURITY NUMBER IS WIDESPREAD 7 (Feb. 1999) [hereinafter USE OF THE SOCIAL SECURITY NUMBER] (citing the advent of computerized databases and efficiency of identification numbers in retrieving and exchanging records for the extensive use of social security number); Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 485-93 (1999).

14. *A National I.D. Card: Big Government at its Worst or Technological Efficiency? Hearing before the Subcomm. on Nat'l Econ. Growth, Natural Resources, and Regulatory Affairs of the House Comm. on Gov't Reform*, 105th Cong. 21 (1998) [hereinafter *National ID Card Hearing*] (statement of Gregory T. Nojeim, Legislative Counsel, American Civil Liberties Union (ACLU)) (referring to the various totalitarian regimes and differentiating the United States where "no American need fear the demand, 'Identity papers!'"); Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 569-70 (1998) (discussing identification numbers as antithetical to democratic ideals and associated with "totalitarian regimes"); *see also* Callahan v. Woods, 658 F.2d 679, 686 (9th Cir. 1981) (holding legitimate a religious fear of the "potential for abuse of the spiritual side of humanity in a number which could act as a universal identifier" (quoting Stevens v. Berger, 428 F. Supp. 896, 905 (E.D.N.Y. 1977)); *cf.* Swire, *supra* note 13, at 495 (discussing Nazi use of personal data collected from Jews to impose a "systematic program" of asset seizure). *Contra* 139 CONG. REC. S11464 (Sept. 10, 1993) (recognizing that many people equate national identification with police states, but believing those analogies misguided); Eric Grossman, Comment, *Conceptualizing National Identification: Informational Privacy Rights Protected*, 19 J. MARSHALL L. REV. 1007, 1009, 1013 (1986) (arguing that modern government must inevitably "dehumaniz[e]" citizens through identification numbers); *cf.* IBM, IBM MULTI-NATIONAL CONSUMER PRIVACY SURVEY 70 (Oct. 2, 1999) [hereinafter CONSUMER PRIVACY SURVEY] (stating that 71% of those surveyed in the United States felt that "it is impossible to protect consumer privacy in the computer age").

15. *Supra* note 13; *see also* Grossman, *supra* note 14, at 1013 ("Prompt and correct administrative action is a direct result of efficiently using and requiring a numerical label.").

individual profile,[16] facilitate efforts to fraudulently assume another's identity,[17] and eliminate bureaucratic impediments to data sharing that previously protected personal privacy.[18]

16. United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 765 (1989) (recognizing that collection of personal information in a database impacts privacy more significantly than summing the danger to privacy posed by pieces of information considered separately); Greidinger v. Davis, 988 F.2d 1344, 1353 (4th Cir. 1993); Aronson v. IRS, 767 F. Supp. 378, 388 (D. Mass. 1991) (denying a Freedom of Information request for taxpayers' social security numbers because that data potentially reveals excessive information about individuals); State *ex rel.* Beacon Journal Publishing Co. v. City of Akron, 640 N.E.2d 164, 169 (Ohio 1994); BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, REPORT TO THE CONGRESS CONCERNING THE AVAILABILITY OF CONSUMER IDENTIFYING INFORMATION AND FINANCIAL FRAUD 8-10 (March 1997); William H. Minor, Note, *Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections*, 28 COLUM. J.L. & SOC. PROBS. 253, 266-68 (1995); *see also* Robert S. Peck, *Extending the Constitutional Right to Privacy in the New Technological Age*, 12 HOFSTRA L. REV. 893, 895 (1984); *cf.* Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint*, WALL ST. J., Apr. 13, 2001, at A1, 2001 WL-WSJ 2860297 (describing the FBI's use of an information reference service that indexes citizen profiles using social security numbers). *But cf. Beacon Journal Publishing Co.*, 640 N.E.2d at 173 (dissenting opinion) (remarking that extensive use of social security numbers in public and private databases indicates that individuals do not have any expectation of privacy for the numbers); Jeff Sovern, *Opting In, Opting Out, or No Options At All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1048-51 (1999) (discussing benefits to consumers from profiling); Fed. Trade Comm'n, *Transcript of Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data* 117-57 (Mar. 13, 2001), *at* http://www.ftc.gov/bcp/workshops/infomkt-place/transcript.pdf (transcribing the testimony from witnesses on the benefits of data exchange and profiling); Direct Marketing Ass'n, *DMA Customer Assistance - Frequently Asked Questions* (last visited Jan. 19, 2000), *at* http://www.the-dma.org/consass5/consasst-faqs5d.shtml (describing the ability of "merge-purge" programs to ensure that consumers are not listed twice on marketing lists).

17. *E.g.*, United States v. Ravitch, 128 F.3d 865 (5th Cir. 1997); *National ID Card Hearing*, *supra* note 14, at 18 (statement of Marvin Young, Jr.) (recounting harm suffered when person engaged in fraudulent credit and criminal activity using Young's name, social security number, and date of birth); OFFICE OF THE INSPECTOR GENERAL, SOCIAL SECURITY ADMIN., ANALYSIS OF SOCIAL SECURITY NUMBER MISUSE ALLEGATIONS MADE TO THE SOCIAL SECURITY ADMINISTRATION'S FRAUD HOTLINE 3-4, A-15-99-92019 (Aug. 1999) [hereinafter MISUSE ALLEGATIONS] (indicating that identity theft allegations constituted 326 of 400 sampled complaints indexed from the 16,375 calls received between October 1, 1997 and March 31, 1999); *see also In re* Crawford, 194 F.3d 954, 958 (9th Cir. 1999); *Beacon Journal Publishing Co.*, 640 N.E.2d at 169. *See generally* FEDERAL TRADE COMM'N, ID THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME (Feb. 2000) (providing consumer information on identity theft).

18. Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1340-41 (1992) (citing statistics regarding the routine computer matches between databases conducted by U.S. government agencies); Swire, *supra* note 13, at 496; *see also* Peck, *supra* note 16, at 895 (discussing networked links between the federal General Services Administration and credit reporting services initiated to investigate people applying for federal loans); *National ID Card Hearing*, *supra* note 14, at 23-24 (statement of Gregory T. Nojeim) (citing specific abuses of social security numbers by the public and private sector perpetrated by culling information from government databases); *cf.* Kathleen A. Linert, Note, *Database Marketing and Personal Privacy in the Information Age*, 18 SUFFOLK TRANSNAT'L L. REV. 687, 690 (1995) ("Information held in computers, as opposed to the old method of paper files, can be more easily collected, accessed more selectively, is cheaper to reproduce, can be transmitted over fax or telephone, and can effortlessly be transferred from one database to another.").

Currently, the United States lacks any national identification number that officially may be used to collate and disseminate personal information on a large scale.[19] The backbone for a national identification number exists, however, due to increasingly sophisticated technology and the social security number's historical development within the context of deficient privacy jurisprudence. The U.S. legal landscape reveals patchwork protections, well below international minimums for data privacy, with egregious loopholes that may be remedied by consulting the national identification approaches in the United Kingdom and South Africa.

A. Current and Emerging Technology[20]

Technological advances leave an indelible mark on society.[21] Increased processing speed, database size, and international network systems form an ocean of information waiting to be harvested. Within this ocean, information regarding specific individuals floats in isolated and disparate masses. Searching by name nets so many superfluous results that it could take hours to verify a subject's information. In contrast, numerical identification permits a search by means so discriminating that it usually only nets the information desired.

Consider a simple database. The user creates a record for every United States citizen. Each record contains fields listing that subject's name, address, and phone number. Once created, anyone with access to the database can query the system with partial or complete information from one field to retrieve the entire record. With only a subject's name and the first three digits of his telephone number, a user could retrieve a full address and complete phone information. Add mapping information to the database, and a user can get directions to the subject's house. The described database only contains information publicly available through telephone directories, but the means by which the database ameliorates the impediments to humans manually collating the information suggests the potential for misuse inherent to large-scale databases.[22]

---

19. *Infra* Part I.B.2.a.i, ii.

20. Focused on describing the reasonable potential for and corresponding risks of database technology, this section will not explore all technological variations and solutions related to databases and identification numbers.

21. Schwartz, *supra* note 18, at 1334-35 ("Characteristics of the computer shape the way that individuals are handled and power is allocated in our country."); George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521, 521-23 (1990); *see also* Swire, *supra* note 13, at 472-77 (detailing behavior-modifying harms to individuals and society that result from financial surveillance).

22. Trubow, *supra* note 21, at 522 ("When committed to paper and trapped within the confines of a manual file, the utility of information is markedly limited."). Several databases exist on the Internet that function similar to the database described. *E.g.*, *555-1212.com* (last visited Jan. 19, 2000), *at* http://www.555-1212.com (allowing user to search by name and location or reverse search by e-mail, phone number, or location); *see also* FEDERAL TRADE COMM'N, TRANSCRIPT OF PUBLIC WORKSHOP ON CONSUMER INFORMATION PRIVACY, SESSION ONE: DATABASE STUDY 31-35 (June 10, 1997) [hereinafter WORKSHOP TRANSCRIPT] (testimony of Timothy Dick, President and CEO, WorldPages) (reverse search info). Most large information reference services adopted self-imposed guidelines that do not allow reverse searches. WORKSHOP TRANSCRIPT, *supra*, at 34-35, 301; *cf.* Indi-

Next, add fields to each record that include financial information,[23] driving history,[24] medical records,[25] criminal records,[26] public records (including marriage, birth, and death certificates),[27] travel log,[28] physical description,[29] DNA,[30] fingerprints,[31] political and religious affiliations,[32] and friends and associates.[33] Although no database currently exists that combines all these fields under a single record, separate databases do exist

---

vidual Reference Services Group, *Industry Principles* (last visited Jan. 19, 2000), *at* http://www.irsg.org/html/industry_principles_principles.htm (principles for information reference services disclosure of information); Direct Marketing Ass'n, *Direct Marketers - DMA Guidelines* (last visited Jan. 19, 2000), *at* http://www.the-dma.org/framesets/dmers/guidelinesframeset.html (principles for direct marketers' collection and use of information).

23. Swire, *supra* note 13, at 464-69 (citing a trend toward private companies, such as banks and credit bureaus, maintaining databases with increasingly detailed and traceable financial transactions); *e.g.*, Steven A. Bibas, Note, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 593-95 (1994).

24. *E.g.*, 49 U.S.C. § 30302 (1999) (originally enacted July 5, 1994, 108 Stat. 973) (establishing the National Driver Register, which tracks individuals whose license has been suspended or revoked or who committed a serious traffic violation); *see also* Nat'l Highway Traffic Safety Admin., *The National Driver Register* (last visited Jan. 19, 2000), *at* http://www.nhtsa.dot.gov/people/perform/driver.

25. *E.g.*, Minor, *supra* note 16, at 254, 279-81.

26. *E.g.*, ZDNet, *DOJ Seeks to Web-enable All Crime Info* (Jan. 17, 2000), *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2423015,00.html (detailing Department of Justice push for a centralized database of criminal records kept by federal, state, local, and tribal governments).

27. *E.g.*, Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1173 (1997) (noting that most states consider marriage, birth, and death certificates public record that can be freely distributed); Brian Krebs, *Privacy Groups, Journalists Clash Over Court Records Database*, NEWSBYTES, Jan. 29, 2001, LEXIS, News Library, NWSBYT File (describing the debates over a proposal to open court records to public Internet searches).

28. *E.g.*, Michael J. AuBuchon, Comment, *Choosing How Safe is Enough: Increased Antiterrorist Federal Activity and Its Effect on the General Public and the Airport/Airline Industry*, 64 J. AIR L. & COM. 891, 894 n.17 (1999) (describing a method for generating airline passenger profiles); *cf.* Matthew Mickle Werdegar, Note, *Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 STAN. L. & POL'Y REV. 103 (1998) (discussing changes in federal regulations that allow location tracking for individuals using cellular phones).

29. Photographs provide a detailed physical description. *E.g.*, Domingo R. Tan, Comment, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP. L.J. 661, 661 n.2 (1999) (referring to a private company collecting photographs from several state motor vehicle agencies).

30. *E.g.*, Dan L. Burk, *DNA Identification Testing: Assessing the Threat to Privacy*, 24 U. TOL. L. REV. 87, 95-96 (1992).

31. *E.g.*, *School Lunch? Let Fingers Do the Paying*, DESERET NEWS, Jan. 25, 2001, LEXIS, News Library, DESNWS File (describing a school lunch program in Pennsylvania that uses fingerprints, instead of cash). *See generally* John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns - Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97 (1997).

32. *E.g.*, HOUSE OF COMMONS, RESEARCH PAPER 93/112 (identifying Greece as compelling citizens to register for an identification card that states the citizen's religion).

33. *E.g.*, Sovern, *supra* note 16, at 1034 n.2 (referring to debtors' use of databases listing neighbors).

that track some of this information.[34]

Networked databases and identification numbers consolidate the disparate information for effortless retrieval by database users. Given the capacity to interlink databases in a network, a user would not need a single, complete database to retrieve records.[35] With simply a name and phone number, networked databases result in an instantaneous subject profile.[36] Introducing identity numbers simplifies the process further for the database user.[37] Assuming assignment of a unique identification number to each subject,[38] users can retrieve information from networked databases without cross-referencing multiple fields to authenticate a subject's identity. Instead of searching through a list of people with a given

34. *Supra* notes 23-33; *see also* Fed. Trade Comm'n, *supra* note 16, at 18-115 (transcribing testimony from witnesses on the breadth of personal data collected by direct marketers and information services and the extent of database sharing between companies); USE OF THE SOCIAL SECURITY NUMBER, *supra* note 13, at 7-8 (noting that one information reference service maintained more than 12,000 "discrete databases" searchable over private networks or the Internet, containing personal information ranging from public records to personal identifying data—name, address, date of birth, and social security number); Simpson, *supra* note 16 (detailing the contents of one information service to include "data ranging from motor-vehicle, driver and boat registrations, liens and deed transfers to phone listings, military records and voter rolls" and recounting the company's claim that "it has records on nearly every American with a credit card"); *cf.* Andrew L. Shapiro, *Privacy for Sale: Peddling Data on the Internet*, NATION, June 23, 1997, LEXIS, News Library, NATION File ("Privacy experts estimate that the average American is profiled in at least twenty-five, and perhaps as many as 100, databases.").

35. *Cf.* Swire, *supra* note 13, at 469 ("In an increasingly networked world, the existence of . . . databases can easily mean that data will spread from one [database] to another.").

36. *Supra* note 16 and accompanying text. As an example, consider two databases. The first database stores the mapping directory for every U.S. citizen, as described in the previous example. The second database stores each citizen's name, address, and physical description. The databases are networked so that information passes freely between them. Instead of culling data from the databases individually, a user with access can submit a single inquiry using a subject's name and address. Since both databases index records by name and address, one system would return the phone number and mapping data, and the other system would return a physical description. The user's computer could combine the information and present the entire result to the user as a single record. From the user's perspective, a name and address would retrieve the corresponding phone number, mapping information, and physical description with a single query.

37. *E.g.*, Grossman, *supra* note 14, at 1012. Phone numbers cannot be considered identity numbers because they are not unique to the individual. The resultant necessity of verification procedures would hamper government and corporate efficiency.

38. *Cf.* Nadine Strossen, *National Health Care: Will Big Brother's Doctor be Watching Us?*, 4 CORNELL J.L. & PUB. POL'Y 438, 442 (1995) (indicating that the social security number is not a good candidate for a national identification number because of the "high percentage of duplicate, fraudulent and inaccurate numbers"); MISUSE ALLEGATIONS, *supra* note 17, at 3-4 (identifying numerous claims of identity theft from a sample of 400 complaints between October 1, 1997 and March 31, 1999); Soc. Security Admin., *The Most Misused Social Security Number of All Time* (last visited Feb. 11, 2000), *at* http://www.ssa.gov/history/misused.html (describing the mass confusion caused by sample social security cards included with wallets). *But cf.* Bowen v. Roy, 476 U.S. 693, 710 (1986) ("Social Security numbers are unique numerical identifiers. . ."); USE OF THE SOCIAL SECURITY NUMBER, *supra* note 13, at 3 ("[T]he SSN has come to be viewed by many as a national identifier because almost every American has an SSN, and each is unique.").

name in a particular city, the user only needs to enter the identification number.[39]

However, technology breeds reliance. During the 1800s, people believed science would provide all the answers to life's problems.[40] That reliance faded, only recently to be replaced by the belief that computers embody the grail of convenience.[41] Revered for an unerring exactitude, computer systems simplify daily tasks and process week-long projects in minutes.[42] Users rely on the seeming perfection of information processed through computers.

As a consequence, assigning identification numbers subordinates the subject's identity to his assigned number and associated database file.[43] Even without the possibility of data entry errors, however, computers do not mirror reality.[44] Once a user introduces identification numbers, reliance on system information threatens the subject's real identity.[45] Ultimately, identification numbers distort reality by reifying database information.[46] In other words, the database information thrives independently of the actual subject described, and the subject's use of his identification number constitutes the only link between reality and the database. If someone obtained the identification number and some supporting information, then that person could appropriate the subject's database iden-

39. For example, consider the simple U.S. mapping directory database. If the user only submits a name to the database, the system retrieves the hundreds of records for people using that name in the United States. If the user queries the system with a name and address, the number of records shrinks considerably. However, numerous records may still exist. Multiple individuals with the same name may live at a given residence or have used the address; for example, a father and son with the same name may live together. To eliminate this multiplicity of records, the user could enter a unique identification number that distinguishes the father and son. Yet, once unique identification numbers are available, the user need not preliminarily narrow results using a name and address. From the initial query, the user could merely submit the identification number to retrieve the desired record.

40. Encyclopædia Britannica, *History of Science* (last visited Jan. 19, 2000), *at* http://www.britannica.com/bcom/eb/article/0/0,5716,117480+13,00.html ("One savant went so far as to express pity for those who would follow him and his colleagues, for they, he thought, would have nothing more to do than to measure things to the next decimal place.").

41. References to the convenience of computers dominate the media, accounting for 554 news accounts in the previous two years. Search of LEXIS, News Library, CURNWS File (Jan. 19, 2000) (search for records containing "convenience w/3 computer").

42. Schwartz, *supra* note 18, at 1335-39 (discussing computers' ability to rapidly process information).

43. *E.g.*, Komuves, *supra* note 14, at 571; Grossman, *supra* note 14, at 1013; *see also* Solove, *supra* note 11 (arguing for an emphasis on the privacy implications raised by the dehumanizing effect of modern information collection).

44. Schwartz, *supra* note 18, at 1339, 1341-43 (warning that the capabilities of computers are limited by the people that enter data and the software programmers).

45. *Supra* note 14.

46. INFO. POL'Y COMM., NAT'L INFO. INFRASTRUCTURE TASK FORCE, OPTIONS FOR PROMOTING PRIVACY ON THE NATIONAL INFORMATION INFRASTRUCTURE, DRAFT FOR PUBLIC COMMENT Part III (April 1997); *see also* Martin Bright, *Identity Cards: A Double-Edged Issue*, GUARDIAN, May 30, 1995, 1995 WL 7606007 ("[I]nformation could be stored and spread without an individual's consent, errors replicated and automatic decisions made about people on the basis of limited information.").

tity.[47] Further, due to the increasing trend toward electronic storage of documents, access to identification numbers provides more information than originally provided by or associated with the identified subject.[48]

Networked database users and subjects may consider these potential difficulties minimal risks, outweighed by the benefits gained through the ability to respond promptly to a subject's needs.[49] An automobile insurance company might monitor the subject's driving history to automatically reduce rates when he maintains a clean record. The State Department could track the purchase of airline tickets to foreign countries and contact individuals with travel advisory information. The Department of Health and Human Services could query medical records to create lists of individuals that need specific vaccinations.[50] Networked databases could provide government or corporate users the capacity to accommodate individual needs in limitless combinations.

Yet, for every hypothetical benevolent use, one can also imagine a malignant abuse of networked databases. Law enforcement officers could retrieve financial or medical information without a search warrant or consent. Airlines could refuse to carry individuals fitting a specific medical or travel profile. Furthermore, anyone with access to the databases could cull information about individuals in need of monetary, medical, or other assistance and utilize that information for financial gain. For example, someone seeking victims to defraud could generate a list of individuals diagnosed with terminal cancer and no surviving family. The infinite beneficial applications for networked databases remain shadowed by the limitless misuses.

Additionally, commentators have noted other concerns considered inherent to uses for large-scale databases and identification numbers, including "mission creep," the chilling effect on subjects' activities, and data security. Mission creep refers to the gradual expansion of data usage for purposes beyond those that justified the initial collection of information.[51] Critics worry about the subject's resultant loss of information con-

47. *E.g.*, *supra* note 17.

48. By querying a document database, a user could search the text of documents for a subject's identification number and retrieve documents and information not available under records indexed by the identification number. *E.g.*, Baker v. Dep't of the Navy, 814 F.2d 1381, 1382-84 (9th Cir. 1987) (limiting the protections of the Privacy Act, *infra* Part I.B.2.a.i, b.i, to records retrievable by "personally identifiable information" and denying plaintiff's claim to amend or purge documents about the plaintiff because the Navy did not index the documents by plaintiff's "personally identifiable information," even though the document would be retrievable by a textual search of the database records).

49. Grossman, *supra* note 14, at 1022-29 ("An analysis of the actual impact of the use of a national identifier, however, indicates that informational privacy is only minimally implicated."); *see also* Schwartz, *supra* note 18, at 1332 (noting the necessity of government information collection to administer services and benefits for citizens).

50. These examples present potential uses of current databases maintained by the government or corporate entities if networked with a proposed audience or recipient for that information.

51. Swire, *supra* note 13, at 497-500 (arguing that economies of scale analysis explains the rationale for expanding database uses but that privacy interests advocate

trol where, for example, an identification number is created to track benefits, but slowly expands to a national identification number that tracks all personal information.[52]

On the other hand, the chilling effect on activities refers to the deleterious influence that information collection and use will have on behavior, as people become better educated about the extent of data usage.[53] Consumers could forego technological options in favor of activities less prone to electronic tracking, or individuals may take special precautions to counteract information collection methods.[54] To stress the detrimental impact on the individual and the system, consider a person that refuses to use the internet out of legitimate tracking concerns[55] or spends an inordinate amount of time developing means to inhibit or avoid data collection.[56] Finally, worries about data security refer to doubts that sufficient security measures exist to protect personal information in databases from unauthorized access. This includes both unofficial use by normal users[57] and illicit retrieval by hackers and crackers.[58]

---

against allowing any extensive use of personal information databases due to the potential "slippery slope"); *see also* Doe v. Herman, No. CIV.A.297CV00043, 1999 WL 1000212, at *9 (W.D. Va. Oct. 29, 1999) (Sargent, Mag. J.) (barring the Department of Labor from claiming that the collection of social security numbers for benefit eligibility purposes justified subsequent use of the numbers as case identifiers for dissemination in hearing notices and published opinions); Strossen, *supra* note 38, at 441-2 ("History is replete with examples of information systems being created for a limited purpose, only to be expanded at a later date.").

52. *Id.*; *see also infra* Part I.B.1 (tracing a similar development in social security numbers).

53. *Supra* note 21 and accompanying text; *see also* Peck, *supra* note 16, at 898-99 ("The chilling effect of a loss of privacy is the undesirable incentive to conform to perceived societal norms rather than assert one's individuality in ways that may threaten to cause a loss in personal or professional associations."); *cf.* Sovern, *supra* note 16, at 1072-73, 1073 n.202 (describing many consumers as unaware of the extent to which businesses use personal information).

54. Swire, *supra* note 13, at 473-75; Rob Carlson, *Rob's Giant BonusCard Swap Meet* (last visited Feb. 23, 2001), *at* http://epistolary.org/rob/bonuscard (making other individual's bar codes available as a means to avoid electronic tracking of food purchases).

55. *E.g.*, John Markoff, *Bit by Bit, Privacy Chipped Away*, AUSTIN AMERICAN-STATESMAN, Mar. 14, 1999, at E1, LEXIS, News Library, AUSTIN File (discussing numbers embedded on computer hardware and software that track movement in cyberspace or facilitate identification on the Internet).

56. Swire, *supra* note 13, at 472-76 (describing various harms incurred by implementing financial surveillance measures).

57. *Id.* at 493-96 (describing reasons why authorized users may access a database improperly); Nina Bernstein, *Lives on File: The Erosion of Privacy*, N.Y. TIMES, June 12, 1997, LEXIS, New Library, NYT File (describing several cases where people with legitimate access to personal information abused that access); Robert Lemos, ZDNet, *Alleged Data Theft by DEA Official Raises Privacy Concerns* (Jan. 24, 2001), *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2677980,00.html (detailing charges against federal official for selling information in law-enforcement databases to private firms); *cf., e.g.*, Romero-Vargas v. Shalala, 907 F. Supp. 1128, 1131 (N.D. Ohio 1995) (Social Security Administration employee failed to follow procedures for disclosure of information).

58. Swire, *supra* note 13, at 496-97 (detailing the methods by which "unauthorized third parties" could gain access to personal information). *See generally* Geek Network, *Glossary, Cracker* (last visited Jan. 20, 2000), *at* http://www.geek.com/glossary/glos-

B. Social Security Numbers

In the abstract, government and corporate use of large-scale databases and identification numbers invokes diverse critical response. However, criticisms of a theoretical database system and identification number only provide background knowledge to evaluate the U.S. and international legal responses to networked databases and national identification numbers. Progressing outside the abstract characterization, the U.S. history of social security numbers provides concrete details of networked databases using identification numbers. Moreover, the legal context surrounding social security numbers raises problems beyond the theoretical risks because U.S. privacy jurisprudence forms a weak patchwork of protections and exemptions to protections.[59] The historical development of this legal context divides into three periods: the expanding use of social security numbers, the rise and fall of privacy, and the time for re-evaluation.

---

sary_search.cgi?cracker (establishing a perceived difference between the labels for people that infiltrate computer systems—hacker and cracker).

59. This Note focuses largely on the Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, and the Supreme Court's recognition of informational privacy, *infra* Part I.B.2. However, several other statutes bear relevance on privacy generally and contribute to the patchwork system currently protecting citizens' personal information. *E.g.*, Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1128 (regulating the collection, use, and dissemination of personal information by consumer credit reporting services); Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, 88 Stat. 571 (mandating accuracy and confidentiality for student records); Right to Financial Privacy Act of 1978, Pub. L. No. 95-630 (prohibiting the disclosure to government officials of personal bank records without a search warrant); Cable Communications Policy Act of 1984, Pub. L. No. 98-549 (barring cable companies from tracking customer habits through personally identifiable information unless the customer consents or tracking is necessary to render service or prevent third party interception); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508 (prohibiting unauthorized interception of any electronic transmission); Video Privacy Protection Act of 1988, Pub. L. No. 100-618 (proscribing disclosure of video rental records with an exception for direct marketing purposes unless customer objects); Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243 (setting groundwork for Federal Communications Commission rule requiring telemarketers to maintain a list of consumers that do not wish to be contacted); Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322 (limiting disclosure of personal information within state motor vehicle databases); Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414 (protecting conversations over cordless phones and requiring that government officials obtain a search warrant before accessing e-mail addresses).

1. *The Expanding Use of Social Security Numbers*[60]

The Social Security Act of 1934[61] initiated the use of social security numbers as a means of maintaining records for citizens qualified to receive benefits.[62] When enacted, politicians specifically commented that the numbers would not be used to implement a national identification system.[63] In 1943, however, President Roosevelt signed an executive order requiring all federal agencies to adopt the social security number if the agency needed an identification system.[64] Despite Roosevelt's recognition of the potential for administrative efficiency through social security numbers,[65] his vision proved premature. Few agencies adopted the social security number prior to the 1970s.[66]

However, three agencies significantly altered the social security number's purpose by adopting the number for identification uses early. In 1961, the Civil Service Commission forced all federal employees to obtain a social security number for use as an employee identification number.[67] The Internal Revenue Service adopted the social security number as a tax identification number for tax returns in 1962.[68] The Department of Defense stopped using service numbers for military personnel in favor of social security numbers in 1967.[69]

As the use of social security numbers spread, an increased danger of disclosure arose after Congress enacted the Freedom of Information Act of

---

60. While this section only describes the steady expansion of social security numbers' use in the public sector, a similar trend existed in the private sector. *E.g.*, IBM, PROTECTING PRIVACY AND SECURING DATA 1-4 (1997); *cf.* Komuves, *supra* note 14, at 536-40 (outlining current uses of the social security number by the private sector). Once social security numbers became more prevalent in the public sector, the private sector had an incentive to use the numbers for identification purposes in corporate databases to facilitate verification and matching with government records. USE OF THE SOCIAL SECURITY NUMBER, *supra* note 13, at 13 (describing the response of corporate interests to proposed federal social security number regulations as strong opposition focused on the need to have some means of exchanging and verifying data with government agencies). Therefore, the expansion in the public sector should also be understood to reflect contemporaneous trends in the private sector.

61. Pub. L. No. 74-271, 49 Stat. 620 (1935).

62. *Id.* § 205 (codified as amended at 42 U.S.C. § 405(c)(2) (1999)).

63. Swire, *supra* note 13, at 499, 499 n.98.

64. Exec. Order No. 9397, 3 C.F.R. 283-84 (1943-1948) (ordering further that the Social Security Board promote the additional federal uses of the social security number by issuing and verifying numbers).

65. Minor, *supra* note 16, at 262; *see also* Schwartz, *supra* note 18, at 1330 (identifying the New Deal era and rise of the "service administration" as the basis of government's need for personal data).

66. *Use of Social Security Number as a National Identifier: Hearing Before the Subcomm. on Social Security of the House Comm. on Ways and Means*, 102d Cong. 23 (1991) (testimony of Gwendolyn S. King).

67. Soc. Security Admin., *Social Security Number Chronology* (last modified Mar. 1, 2000), *at* http://www.ssa.gov/history/ssnchron.html [hereinafter *Chronology*].

68. Internal Revenue Code Amendments, Pub. L. No. 87-397, 75 Stat. 828 (1961) (codified as amended at 26 I.R.C. § 6109 (1999)); *see also* Minor, *supra* note 16, at 263 n.55.

69. *Chronology*, *supra* note 67.

1966,[70] which granted citizens access to information held by government agencies. Subsequently, in 1970, Congress legislated a mandatory scheme for private banks and other financial institutions to obtain customers' social security numbers.[71] Social security numbers had expanded far beyond their original purpose to track earnings for social security benefits and rapidly neared use as national identification numbers.

2. *The Rise and Fall of Privacy*

The first sign of significant concern for privacy appeared in an agency report recommending a more "cautious" approach to adopting social security numbers as identification numbers.[72] A later report criticized the need for national identification cards and rejected social security numbers as unsuitable for unique identifiers.[73] Between reports, however, Congress enacted legislation further expanding the use of social security numbers.[74] Finally, Congress focused on curtailing government collection and use of social security numbers through the Privacy Act of 1974.[75]

a. The Rise of Privacy

i. Privacy Act of 1974

The Privacy Act prohibited local, state, and federal government agencies from denying benefits to citizens based on a refusal to submit a social security number, unless a statute mandated collection of social security numbers or the government program had used the numbers for identification before 1975.[76] Furthermore, the Privacy Act ordered any state or federal agency requesting a social security number to notify the individual whether revealing the number was voluntary.[77] The statute mandated that the agency indicate any statutory authority requiring collection of the number and how they would use the number.[78] Finally, the Privacy Act required agencies to obtain written consent from individuals prior to dis-

70. Pub. L. No. 89-487, 80 Stat. 250. *But see* Aronson v. IRS, 767 F. Supp. 378 (D. Mass. 1991) (exempting disclosure of social security numbers from a Freedom of Information request due to privacy concerns); Komuves, *supra* note 14, at 555-56 (discussing judicial protection against social security number disclosure based on exemption six of the Act for a "clearly unwarranted invasion of personal privacy"). *See generally* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 592-95 (1995) (exploring the interaction between the Privacy Act, the Freedom of Information Act, and personal information).

71. Bank Secrecy Act, Pub. L. No. 91-508 (1970).

72. SOC. SECURITY NUMBER TASK FORCE, SOC. SECURITY ADMIN., REPORT TO THE COMMISSIONER (1971).

73. U.S. DEP'T. OF HEALTH, EDUC. AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973); *see also supra* note 38.

74. Social Security Amendments of 1972, Pub. L. No. 92-603 (codified as 42 U.S.C. 405) (requiring legal aliens and anyone receiving federal benefits to obtain a social security number).

75. Pub. L. No. 93-579, 88 Stat. 1896.

76. *Id.* § 7(a).

77. *Id.* § 7(b) (codified as amended at 5 U.S.C. § 552a(e)(3)(A) (1999)).

78. *Id.* (codified as amended at 5 U.S.C. § 552a(e)(3)(B) (1999)).

closing collected information to other sources.[79] However, disclosure without consent was possible if it fell within twelve exceptions.[80]

Congress recognized the inherent dangers of large-scale databases and identification numbers and sought to establish guidelines for the collection, use, and dissemination of records in government databases.[81] Congress intended the guidelines to ensure that each user has a legitimate purpose, information remains accurate, and security measures protect data from unauthorized access.[82] Further, Congress sought to confer privileges upon every citizen to retrieve, control, and correct their personal information and initiate a civil suit for intentional violations by federal agents.[83] Congress considered these protections, guidelines, and privileges absolute unless statutory authority outlined significant public policy arguments limiting their scope.[84] Three years later, a study mandated by the Privacy Act[85] cautioned against development of a national identification number

79. *Id.* § 3 (codified as amended at 5 U.S.C. § 552a(b) (1999)).

80. (1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
(2) required under section 552 of this title;
(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;
(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;
(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;
(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;
(11) pursuant to the order of a court of competent jurisdiction; or
(12) to a consumer reporting agency in accordance with section 3711(e) of title 31.

Id.

81. *Id.* § 2 (Congressional findings and statement of purpose). *See generally supra* Part I.A.

82. Privacy Act of 1974, Pub. L. No. 93-579, § 2, 88 Stat. 1896.

83. *Id.*

84. *Id.*

85. *See id.* § 5.

until further analysis of the Privacy Act's effectiveness could be ascertained.[86]

ii. Informational Privacy

Contemporaneous to passage of the Privacy Act, a constitutional right to privacy was developed with implications for the use of government databases storing personal information. This right to privacy jurisprudence originated in a dissent.[87] In *Olmstead v. United States*, the majority upheld the admissibility of wiretapping evidence in a Prohibition-era alcohol-distribution conspiracy, despite Fourth and Fifth Amendment challenges.[88] However, Justice Brandeis argued in dissent that the narrow language of the Fourth Amendment encompassed a broad protection.[89] Advocating recognition of a right to privacy, Brandeis relied on the philosophical values motivating passage of the Fourth Amendment and focused on the desire to protect freedom from government interference.[90]

After thirty-seven years, the Supreme Court invoked a nebulous interpretation of the Constitution to justify a right to privacy.[91] In *Griswold v. Connecticut*, the Court held that a right to privacy exists that protects a married couple's use of contraceptives from government intrusion.[92] The Court applied an analysis similar to Brandeis's reliance on values not explicitly stated in the Constitution.[93] Basing its holding on the principles underlying the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments, the Court recognized the values of the Bill of Rights as establishing "zones of privacy" that required constitutional protection.[94]

Subsequently, the Court examined these zones and constrained the right to privacy to interests deemed "fundamental" or "implicit in the concept of ordered liberty."[95] Then, in *Paul v. Davis*, the Court confronted the privacy interests implicated by public officials' disclosure of personal information.[96] In *Davis*, the Chief of Police circulated a photograph of Davis on a list of "active shoplifters," based on Davis's arrest for a charge that had

86. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) [hereinafter PRIVACY STUDY].

87. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("The protection guaranteed by the Amendments is much broader in scope . . . . They conferred, as against the Government, the right to be let alone."); *cf.* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (setting a foundation for the concepts that Brandeis would later introduce in his dissent).

88. 277 U.S. 438.

89. *Id.* at 478 (Brandeis, J., dissenting).

90. *Id.*

91. Griswold v. Connecticut, 381 U.S. 479 (1965).

92. *Id.*

93. *Compare id.* at 484-85, *with Olmstead*, 277 U.S. at 478 (Brandeis, J., dissenting). This approach to constitutional interpretation has been severely criticized. *Griswold*, 381 U.S. at 510 (Black, J., dissenting). *But see* Peck, *supra* note 16, at 903-05.

94. *Griswold*, 381 U.S. at 485.

95. Roe v. Wade, 410 U.S. 113, 152-53 (1973) (citing Palko v. Connecticut, 302 U.S. 319, 325 (1937)); *see also* Gary R. Clouse, Comment, *The Constitutional Right to Withhold Private Information*, 77 NW. U. L. REV. 536, 531 n.34 (1982).

96. 424 U.S. 693 (1976).

been dismissed prior to the list's distribution.[97] The Court relied on the limited scope of the right to privacy to conclude that the right only protected information related to "fundamental" activities.[98] Expounding on this fundamental rights analysis, the Court confined the activities largely to "marriage, procreation, contraception, family relationships, and child rearing and education."[99] Applying the test, the Court concluded that the arrest information did not qualify as a fundamental activity.[100]

However, as computers became more prevalent and social security numbers requisite, another Supreme Court dissent set the foundation for a parallel line of cases to the right to privacy.[101] In a 1974 challenge to the Bank Secrecy Act,[102] Justice Douglas argued that citizens have a privacy interest against disclosure of information that potentially reveals intimate details of their lives, such as the mandatory social security number disclosure under the Act.[103] Furthermore, Douglas contended that citizens have a legitimate expectation of privacy in bank account information to preclude a bank's disclosure of personal information to the government.[104]

In 1977, with a tension between the *Davis* case and Douglas's dissent, the Court decided the constitutionality of a state statute requiring disclosure of prescriptions for specified drugs.[105] In *Whalen v. Roe*,[106] the Court avoided the need for a fundamental activity analysis by characterizing the right to privacy as protecting two distinct interests, "avoiding disclosure of personal matters" and "independence in making certain kinds of important decisions."[107] The Court acknowledged Douglas's dissent in discussing the first branch of the right to privacy.[108] Yet, to resolve the tension, the Court recognized *Davis* as controlling for the second branch. The Court evaded the fundamental activity analysis by establishing the distinction, but proceeded to uphold the statute as posing no significant threat to privacy.[109] The Court's distinction, however, failed to address the appar-

97. *Id.*
98. *Id.* at 712-13 (citing *Palko*, 302 U.S. at 325).
99. *Id.* at 713.
100. *Id.*
101. California Bankers Ass'n v. Shultz, 416 U.S. 21, 79 (1974) (Douglas, J., dissenting), *cited with approval in* Whalen v. Roe, 429 U.S. 589, 599 n.25 (1977) (using *California Bankers* to support a holding that constitutional privacy recognizes an "individual interest in avoiding disclosure of personal matters"); *see also* Doe v. McMillan, 412 U.S. 306, 329 (1973) (Douglas, J., concurring) (expressing alarm at the dangers of networked databases and social security numbers' use).
102. Pub. L. No. 91-508 (1970); *see also supra* note 71 and accompanying text.
103. *Id.*; *California Bankers*, 416 U.S. at 85-86 (Douglas, J., dissenting).
104. *California Bankers*, 416 U.S. at 88-89 (Douglas, J., dissenting).
105. Whalen v. Roe, 429 U.S. 589 (1977).
106. *Id.*
107. *Id.* at 599-600.
108. *Id.* at 599 n.25.
109. *Id.*; *see also* Nixon v. Adm'r of Gen. Servs., 433 U.S. 425, 457-59 (1977) (applying the distinction and weighing the importance of the President's privacy interest and reasonable expectation of privacy against the public interest in disclosure). Neither case explicitly adopts a balancing approach to informational privacy, but the applied analysis indicates a weighing of factors. *Id.*; Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Pri-*

ent factual tension between the *Whalen* holding and *Davis*, which rejected a privacy interest in avoiding disclosure based on the fundamental activity analysis.[110] The Court set adrift this uncertain notion of informational privacy and failed to return significantly to the subject.[111]

b. The Fall of Privacy

i. Privacy Act of 1974

Unfortunately, the legislature failed to sustain the promising spirit of the strongly worded Privacy Act. Congress failed to rectify significant loopholes in the privacy regulations and started to enact statutes that created piecemeal exemptions for federal agencies and state programs. Three regulatory gaps in the Privacy Act of 1974 severely limited the strength of the protections. First, the statute utterly failed to restrict the practices of corporate entities or confer upon individuals any right of action against state or local governments that violate the protections;[112] only a federal executive or independent regulatory agency would be subject to citizen suits for violations.[113] Even against federal agencies, the remedies remained limited to administrative injunctions and minimal damages.[114] Second, an exception for agencies using systems of records prior to 1975 exempted an extensive array of uses.[115] Third, a "routine use" clause for disclosure

---

vacy, 10 N. ILL. U. L. REV. 479, 504 n.88, 508-09 (1990); *see also* Clouse, *supra* note 95, at 545-47; *infra* Part I.B.2.b.ii (examining the subsequent standards applied in Courts of Appeals); *cf.* Grossman, *supra* note 14, at 1024-25 (assuming a balancing inquiry to evaluate informational privacy claims).

110. *Compare* Paul v. Davis, 424 U.S. 693, 713 (1976), *and infra* Part I.B.2.b.ii (referring to some Courts of Appeals that rely on *Davis* to minimize the impact of *Whalen*), *with Whalen*, 429 U.S. at 599-600.

111. One case discussed the holding of *Whalen* in detail. United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 769-71 (1989). However, the discussion was background on U.S. privacy jurisprudence to resolve a construction of privacy as an exemption for the Freedom of Information Act. *Id.* at 762-71; *see also* Cutshall v. Sundquist, 193 F.3d 466, 481 (6th Cir. 1999) (referring to "any reference in [*Reporters Committee*] made to this possible right [to avoid public disclosure of information as] was mere dicta"); *cf. supra* note 70. Therefore, it is doubtful the Court would consider the analysis binding precedent since it was not central to the case's holding. *Reporters Committee*, 489 U.S. at 762 n.13.

112. *See* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896; Dittman v. California, 191 F.3d 1020, 1027 (9th Cir. 1999); Polchowski v. Gorris, 714 F.2d 749, 752 (7th Cir. 1983); Komuves, *supra* note 14, at 550, 569.

113. *Id.*; 5 U.S.C. § 552(f) (1999) (defining agencies subject to civil action under the Privacy Act).

114. 5 U.S.C. § 552a(g); Schwartz, *supra* note 70, at 587 (referring to the inadequacy of the authorized remedies to control agency behavior); *see also* Komuves, *supra* note 14, at 553-54.

115. Given Roosevelt's Executive Order, *supra* note 64 and accompanying text, the exception for identification systems prior to 1975 exempted many federal agencies. Brookens v. United States, 627 F.2d 494, 497-98 (D.C. Cir. 1980) (upholding the Executive Order as authority sufficient to exempt an agency from Privacy Act restrictions). The Privacy Protection Study Commission authorized by the Privacy Act recommended legislation to revoke the Executive Order as authorization for agencies to continue using social security numbers, but Congress never acted on the recommendation. PRIVACY STUDY, *supra* note 86.

regulations became a catch-all agency exemption.[116]

In addition to these integrated exceptions, Congress initiated a march of wholesale exemptions for specific government programs.[117] In 1976, Congress granted state and local agencies permission to use social security numbers for taxes, welfare, and driver's licenses and motor vehicle registrations.[118] Over the next sixteen years, Congress enacted a series of acts mandating social security number disclosure for individuals receiving government benefits or services.[119] Despite the expansive use of social security numbers for identification, reports by several advisory committees and statements by successive Presidents continued to decry proposals for national identification numbers.[120]

In 1996, Congress stepped significantly toward a national identification card by requiring social security numbers for a diverse range of public

116. Schwartz, *supra* note 70, at 584-87 (describing criticism that agencies exploit the "routine use" exemption, but noting the inability to change agency conduct due to the limited remedies enforceable by courts). *Contra* Doe v. Herman, No. CIV.A.297CV00043, 1999 WL 1000212, at *11 (W.D. Va. Oct. 29, 1999) (Sargent, Mag. J.) (enforcing strictly the statutory requirement that "routine uses" be published in the Federal Register).

117. *E.g.*, Komuves, *supra* note 14, at 550 ("[W]hen one considers how many exceptions Congress has granted for SSN collection and use, the exceptions clearly swallow the general rule."). However, in 1990, Congress granted a respite from the onslaught of Privacy Act exceptions by addressing a failure to regulate automated database comparisons between government agencies. Computer Matching and Privacy Protection Amendments of 1990, Pub. L. No. 101-508 (codified as amended at 5 U.S.C. § 552a (1999)); *see also* Schwartz, *supra* note 70, at 587-89 (discussing the benefits and shortcomings of the amendments). The amendments imposed procedural safeguards on agencies matching database information with other government entities. *Id.* The Act required agencies to obtain written matching agreements with the other agency involved that specified the match's purpose, cost, benefit, and description. Computer Matching and Privacy Protection Amendments of 1990, Pub. L. No. 101-508 (codified as amended at 5 U.S.C. § 552a(o) (1999)). Further, prior to adverse action regarding government benefits, the amendments required agencies to verify information or notify persons matched and offer an opportunity to be heard regarding errors. *Id.* (codified as amended at 5 U.S.C. § 552a(p) (1999)). Finally, the amendments mandated the creation of Data Integrity Boards within the agencies to oversee matching programs and required agencies to submit a report to the Office of Management and Budget and two Congressional committees prior to initiating any new matching programs. *Id.* (codified as amended at 5 U.S.C. § 552a(r), (u) (1999)).

118. Tax Reform Act of 1976, Pub. L. No. 94-455, (codified as amended at 42 U.S.C. § 405(c)(2)(C)(i) (1999)); *see also* Deficit Reduction Act of 1984, Pub. L. No. 98-369 (permitting State use of social security numbers for Aid to Families with Dependent Children, Medicaid, unemployment compensation, and food stamp programs); Technical and Miscellaneous Revenue Act of 1988, Pub. L. No. 100-647 (blood donation programs); Social Security Independence and Program Improvements Act of 1994, Pub. L. No. 103-296 (jury selection).

119. Food Stamp Act of 1977, Pub. L. No. 96-58 (requiring social security number disclosure to enroll in food stamps program); Debt Collection Act of 1982, Pub. L. No. 97-365 (federal loans); Higher Education Amendments of 1986, Pub. L. No. 99-498 (student loans); Housing and Community Development Act of 1987, Pub. L. No. 100-242 (Housing and Urban Development programs); Family Support Act of 1988, Pub. L. No. 100-485 (parents' social security numbers for birth certificates).

120. *Chronology*, *supra* note 67 (citing reports by the Federal Advisory Committee on False Identification and the Privacy Protection Study Commission and statements by the Carter and Reagan administrations).

records.[121] It also set mandatory standards for identity verification by federal agencies, requiring social security numbers on identification documents.[122] After refusing to appropriate funds for the Department of Transportation to implement the new identification standards,[123] Congress repealed the social security number requirement in October 1999.[124] Although avoiding egregiously overt measures, Congress has established covertly a de facto national identification number by enacting exceptions to the Privacy Act. For every step toward respecting an individual's privacy,[125] Congress retreated two steps in subsequent legislation.[126]

ii. Informational Privacy

Even as Congress muddled the Privacy Act, the judiciary failed to uniformly sustain the concept of informational privacy. Soon after the recognition of an individual's privacy interest in avoiding disclosure of information—the confidentiality branch of the right to privacy,[127] courts acknowledged two stages in information transfers that implicate the privacy interest: individuals' release of information to the government and the government's public release of collected information.[128] For example, in *Barry v. City of New York*, the Second Circuit analyzed separately the constitutional implications for clauses requiring public officials to file financial information with the state government and provisions allowing public inspection of those documents.[129] Adding a further complication, the Supreme Court expressed reluctance to acknowledge categories of substantive rights beyond fundamental rights in "matters relat[ed] to marriage, family, procreation and the right to bodily integrity."[130]

121. Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193 (requiring social security numbers for any professional license, commercial driver's license, occupational license, marriage license, divorce decree, child support order, paternity judgment, or death certificate).

122. Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, Div. C, Title VI, Subtitle D, § 656, 110 Stat. 3009-716 (codified as amended at 5 U.S.C. § 301 note (1999)) (permitting also the Attorney General to require social security numbers from any noncitizen, § 415).

123. Department of Transportation and Related Agencies Appropriations Act, Pub. L. No. 105-277, Div. A, § 101(g), Title III, § 362 (1998).

124. Department of Transportation and Related Agencies Appropriations Act, Pub. L. No. 106-69, § 355, 113 Stat. 986, 1027 (2000).

125. *Supra* Part I.B.2.a.i, note 109.

126. *Supra* notes 112-22 and accompanying text.

127. *See* Plante v. Gonzalez, 575 F.2d 1119, 1132 (5th Cir. 1978).

128. *E.g.*, Barry v. City of New York, 712 F.2d 1554, 1559-64 (2d Cir. 1983); *see also* Grossman, *supra* note 14, at 1014 & n.48, 1024-28. Unlike the legislative side of U.S. privacy jurisprudence, the courts considering constitutional challenges are limited to cases of state action. In most instances of corporate collection and disclosure, any connection to relevant government activity would be too attenuated to establish state action. Therefore, even if a strong right to informational privacy existed in the Constitution, it would not cover many of the transactions that implicate privacy interests in the information age.

129. 712 F.2d at 1559-64.

130. Albright v. Oliver, 510 U.S. 266, 271-72 (1994); *cf. supra* notes 95-100 and accompanying text (noting the initial stages of the trend away from recognizing new fundamental rights).

Due to the minimal and mixed guidance from the Supreme Court,[131] the Courts of Appeals formulated a balancing test for a right to confidentiality.[132] While the tests differ across Circuits,[133] most Circuits validate the privacy interest in confidentiality by applying a threshold test, requiring proof that the individual seeks to protect "intimate" or "personal" information[134] or information subject to an expectation of confidentiality or privacy.[135] Satisfying the threshold, the validated privacy interest is weighed against the government interest in disclosure.[136] Although the Supreme Court's inconsistent statements influenced some courts to restrict the

131. American Fed'n of Gov't Employees v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 791 (D.C. Cir. 1997) (remarking that the Supreme Court has made references to a right of information privacy in dicta, but never resolved the issue); *Barry*, 712 F.2d at 1559 ("The nature and extent of the interest recognized in *Whalen* . . . are unclear."); *Plante*, 575 F.2d at 1134; *see also supra* note 111 and accompanying text. *Compare supra* Part I.B.2.a.ii (detailing the rise of information privacy separate from a reliance on an analysis of traditional rights in fundamental activities), *with supra* note 130 and accompanying text (describing the trend toward denying any rights not related to fundamental activities).

132. Ferguson v. City of Charleston, S.C., 186 F.3d 469, 477 (4th Cir. 1999); Eagle v. Morgan, 88 F.3d 620, 625 (8th Cir. 1996); Harris v. Thigpen, 941 F.2d 1495, 1513 n.26 (11th Cir. 1991); Flanagan v. Munger, 890 F.2d 1557, 1570 (10th Cir. 1989); Daury v. Smith, 842 F.2d 9, 13-14 (1st Cir. 1988); Pesce v. J. Sterling Morton High Sch., 830 F.2d 789, 797-98 (7th Cir. 1987); *Barry*, 712 F.2d at 1559; United States v. Westinghouse Elec. Corp., 638 F.2d 570, 578-79 (3d Cir. 1980); *Plante*, 575 F.2d at 1134; *see also* Turkington, *supra* note 109, at 504-09 (exploring the scope of information privacy through a balancing test); *cf. American Fed'n of Gov't Employees*, 118 F.3d at 793 (refusing to rule on the existence of a right to information privacy, but, under the assumption that the right exists, applying a balancing test); Russell v. Gregoire, 124 F.3d 1079 (9th Cir. 1997) (avoiding the issue whether a right to information privacy exists, but limiting any right to only personal information). *Contra* J.P. v. DeSanti, 653 F.2d 1080, 1088-89 (6th Cir. 1981) (declining to recognize a right to information privacy from *Whalen* and applying the strict fundamental rights test).

133. *Pesce*, 830 F.2d at 797 n.5.

134. *E.g.*, Powell v. Schriver, 175 F.3d 107, 111 (2d Cir. 1999) ("The excruciatingly private and intimate nature of transsexualism, for persons who wish to preserve privacy in the matter, is really beyond debate."); Doe v. Plymouth, 825 F. Supp. 1102, 1107 (D. Mass. 1993) ("There are few areas which more closely intimate facts of a personal nature than one's HIV status.").

135. *E.g.*, Paul P. v. Verniero, 170 F.3d 396, 401 (3d Cir. 1999) ("[I]n determining whether information is entitled to privacy protection, we have looked at whether it is within an individual's reasonable expectations of confidentiality." (quoting Fraternal Order of Police v. Philadelphia, 812 F.2d 105, 112-13 (3d Cir. 1987)); *Eagle*, 88 F.3d at 625 ("To determine whether a particular disclosure [exposes information "representing 'the most intimate aspects of human affairs'"], we must . . . assess whether the person had a legitimate expectation that the information would remain confidential . . . ."); Walls v. Petersburg, 895 F.2d 188, 192 (4th Cir. 1990); *Flanagan*, 890 F.2d at 1570.

136. *E.g.*, *Powell*, 175 F.3d at 111-13 (implicitly balancing a privacy interest in concealing gender identity with public interest in orderly regulation of prisons); *Westinghouse Elec. Corp.*, 638 F.2d at 578 (detailing a list of factors for consideration including information to be disclosed, potential harm from disclosure, security protections for disclosed information, public need for information, and public policy or other legislative mandates); Doe v. Plymouth, 825 F. Supp. at 1107-08 (stating that the First Circuit has not ruled on the scope or existence of a right to confidentiality, but polling other circuits to adopt a balancing test).

scope of information privacy to fundamental activities,[137] most Circuits recognize and enforce the right to confidentiality.[138]

While different balancing tests result in a less uniform blanket of protection, the differences pose no significant threat. A more serious concern stems from courts uncritical reliance on precedent despite technological advances that negate the precedent's reasoning. Although concerns about information collection in databases existed prior to 1988,[139] the Computer Matching and Privacy Protection Act[140] set a framework for understanding and evaluating the privacy implications for networked databases.[141] Given Congress's recognition of a shift in the technological landscape, courts evaluating expectations of privacy should examine cases decided prior to that shift. While Justice Douglas noted with disapproval the use of social security numbers with networked databases in 1971,[142] several pre-1988 cases ruled that social security numbers' use does not threaten an individual's privacy.[143] In contrast, since 1988, courts increasingly recognize the privacy risks inherent in disclosing social security numbers.[144]

Unfortunately, some courts continue to rely on cases decided prior to 1988 without analyzing the underlying rationale.[145] This uncritical approach poses an especially significant threat because the commonly cited case,[146] *McElrath v. Califano*,[147] provides no reasoned analysis to sup-

137. *E.g.*, J.P. v. DeSanti, 653 F.2d at 1088-89 (denying any right to confidentiality and applying fundamental matters analysis); *Ferguson*, 186 F.3d at 482 (recognizing a right to confidentiality, but applying the fundamental matters analysis as a threshold requirement).

138. *Supra* note 132 (listing only the Sixth Circuit as refusing to recognize a right of confidentiality and the Ninth Circuit and D.C. Circuit as avoiding any stance on the right's existence).

139. *E.g.*, *supra* note 81 and accompanying text.

140. Pub. L. No. 100-503, 102 Stat. 2507 (1988) (codified as amended at 5 U.S.C. § 552a (1999)).

141. *Supra* note 117.

142. Doe v. McMillan, 412 U.S. 306, 325 (1973) (Douglas, J., concurring).

143. McElrath v. Califano, 615 F.2d 434, 441 (7th Cir. 1980); Doyle v. Wilson, 529 F. Supp. 1343, 1348 (D. Del. 1982); Greater Cleveland Welfare Rights Org. v. Bauer, 462 F. Supp. 1313, 1318-19 (N.D. Ohio 1978). *But cf. supra* Part I.A. (explaining the dangers inherent to national identification numbers and networked databases).

144. *In re* Crawford, 194 F.3d 954, 958-59 (9th Cir. 1999); Greidinger v. Davis, 988 F.2d 1344, 1353 (4th Cir. 1993); Int'l Bhd. of Elec. Workers v. United States Dep't of Hous. & Urban Dev., 852 F.2d 87, 88-89 (3d Cir. 1988); Doe v. Herman, No. CIV.A.297CV00043, 1999 WL 1000212, at *7-8 (W.D. Va. Oct. 29, 1999) (Sargent, Mag. J.); Oliva v. United States, 756 F. Supp. 105, 107 (E.D.N.Y. 1991); Tribune-Review Publishing Co. v. Allegheny County Hous. Auth., 662 A.2d 677, 681 (Pa. Commw. Ct. 1995); State *ex rel.* Beacon Journal Publishing Co. v. City of Akron, 640 N.E.2d 164, 167-69 (Ohio 1994); *cf.* Walls v. Petersburg, 895 F.2d 188, 194-95 (4th Cir. 1990) ("[T]echnological advances have provided society with the ability to collect, store, organize, and recall vast amounts of information about individuals in sophisticated computer files . . . . [W]e need to be ever diligent to guard against misuse.").

145. *E.g.*, Claugus v. Roosevelt Island Hous. Management Corp., No. 96CIV8155(MJL)(KTD), 1999 WL 258275, at *7 (S.D.N.Y. Apr. 29, 1999); *In re* Rausch, 213 B.R. 364, 367 (Bankr. D. Nev. 1997); *In re* Turner, 193 B.R. 548, 553 (Bankr. N.D. Cal. 1996).

146. *Id.*

147. 615 F.2d 434.

port its denial of privacy claims.[148] Ruling in 1980, the Seventh Circuit relied on a fundamental rights analysis for privacy claims stemming from refusals to disclose social security numbers as a condition on welfare benefits.[149] The court did not consider the impact of *Whalen* on the right to privacy[150] or the Privacy Act on claims related to social security numbers.[151] Ignoring technological advances, some courts have refused to consider privacy claims for social security numbers by blindly relying on outdated opinions that lack a sustainable rationale.

3. The Time for Re-evaluation

In sum, courts apply U.S. privacy protections haphazardly. Procedural deficiencies allow government and corporate abuses that invade personal privacy. Recent policy efforts to address identified deficiencies inadequately protect individuals, and that failure highlights the need to consider new strategies for protecting personal information. Meanwhile, renewed congressional concern for privacy demonstrates that the political climate is preparing for changes; the only issue will be the degree of protection afforded citizens.

One criticism of United States privacy protections that commentators and agencies raise consistently is the lack of comprehensive regulation.[152] The critiques focus on the failure to regulate private entities.[153] In most cases, individuals need not reveal their social security number to private organizations.[154] Yet, no legislation bars the entities from requesting personal information for their databases.[155] When confronted with a private group requesting unnecessary or superfluous personal information, an individual's only remedy is patronizing a competing business, hoping the same policy does not pervade the entire industry.[156] The extensive list of government exemptions for collection and use of social security numbers[157] exacerbates the problem because the number presents a tempting

148. *Id.* at 441.

149. *Id.*; *see also supra* notes 95-96 and accompanying text.

150. *Compare McElrath*, 615 F.2d at 441, *with supra* notes 107-09 and accompanying text.

151. *Compare McElrath*, 615 F.2d at 441, *with supra* Part I.B.2.a.i.

152. USE OF THE SOCIAL SECURITY NUMBER, *supra* note 13, at 4; Komuves, *supra* note 14, at 550, 569.

153. *Id.*

154. *E.g.*, SOC. SECURITY ADMIN., YOUR NUMBER AND CARD, PUB. NO. 05-10002 (April 1999) [hereinafter YOUR NUMBER]; Computer Professionals for Social Responsibility, *SSN FAQ: Private Requests for your SSN* (last modified Feb. 11, 2001), *at* http://www.cpsr.org/cpsr/privacy/ssn/SSN-Private.html (detailing private entities to whom individuals must reveal social security numbers); Privacy Rights Clearinghouse, *Fact Sheet #10: Your Social Security Number: How Secure Is It?* (last visited Oct. 24, 1999), *at* http://www.privacyrights.org/fs/fs10-ssn.htm.

155. *Id.*

156. YOUR NUMBER, *supra* note 154; Chris Hibbert, Computer Professionals for Social Responsibility, *History and Significance of the Social Security Number* (last modified April 24, 1999), *at* http://www.cpsr.org/cpsr/privacy/ssn/SSN-History.html#protect (describing steps available for dealing with corporate requests for social security numbers, from supplying other forms of identification to seeking services or goods elsewhere).

157. *Supra* notes 112-21 and accompanying text.

means of verification for private groups seeking to cross-reference data with government databases.[158]

Stating that "the United States has adopted a comprehensive approach to limiting the Government's collection, use and disclosure of personal information," President Clinton issued a policy statement to executive agencies that espoused a spirit of heightened awareness in protecting the privacy of citizens' information contained in government records.[159] The memorandum and subsequent Office of Management and Budget (OMB) instructions required each agency to assign a senior official as primary agent for privacy issues, review existing systems and proposed legislation for privacy implications, and submit a summary report to the OMB.[160] The President's memorandum articulates a sentiment for policing government practices to minimize invasion of personal privacy. If databases are shielded by privacy restrictions, corporate entities and other government agencies lose the efficiency value gained through profiling across separate databases using identification numbers.[161]

Although not completed,[162] the tasks set in the President's memoran-

158. *See generally* USE OF THE SOCIAL SECURITY NUMBER, *supra* note 13, at 7-12 (specifying the various uses of social security numbers by private entities and identifying a primary motivation for collection of numbers as "conduct[ing] data exchanges with other organizations").

159. Privacy and Personal Information in Federal Records, M-99-05, Attachment A (May 14, 1998) [hereinafter Privacy Memo].

160. *Id.* at Attachment A, B.

161. *Supra* notes 13, 35-36, 49-50, 60, 158 and accompanying text (describing the conveniences and efficiency of profiling through networked databases).

162. While many agencies filed their required reports with the OMB, the OMB has not released a summary of the agencies' findings. The summary will be critical to evaluating the extent of agency compliance with existing privacy protections and existing agency uses of personal information. At least one commentator has argued that agencies manipulate loopholes in the Privacy Act and fail to carefully maintain adequate use descriptions in the Federal Register. Schwartz, *supra* note 70, at 584-89 (describing methods through which agencies circumvent privacy protections); *see also supra* Part I.B.2.a.i, b.i (discussing loopholes in the Privacy Act and use registration requirements for the Computer Matching and Privacy Protection Act). Courts perpetuate agency attitudes that violate the spirit of the privacy protections by deferring to agency interpretation of rules promulgated pursuant to the statutes. The courts will not defer to an agency's statutory interpretation, but courts will defer to agency interpretation of routine use exceptions under the Privacy Act. *Compare* Ass'n of American Physician and Surgeons, Inc. v. Clinton, 997 F.2d 898, 913 (D.C. Cir. 1993) (declining to defer to agency interpretation of statutes that apply to more than one agency), *with* NLRB v. USPS, 128 F.3d 280, 284 n.3 (5th Cir. 1997) (deferring to agency interpretation of self-promulgated routine use because "analysis of [the] Routine Use . . . requires interpretation of neither the common law nor constitutional law and therefore, deference to the Board's reasonable interpretation is appropriate"), *and* Dep't of the Air Force v. FLRA, 104 F.3d 1396, 1401-02 (D.C. Cir. 1997). *Cf.* USPS v. Nat'l Ass'n of Letter Carriers, 9 F.3d 140 (D.C. Cir. 1993) (deferring to an arbitrator's interpretation of agency's routine use provision that held detailed employee personal information, including "name and social security number . . . sex; date of birth; minority status code; handicap status code; veteran preference status code; life insurance status code; thrift savings plan status code; thrift savings plan deduction—percent; and thrift savings plan deduction—amount," was "needed by [a labor] organization to perform properly its duties as the collective bargaining representative").

dum will fail to culminate in any radical solution to the critique of inadequate regulation. First, the memorandum declares that "comprehensive" regulation exists, but bases that assertion on the statutes and principles that only provide patchwork protections.[163] Even if the memorandum imposed duties on agencies beyond those set out by statute, the President specified that individuals retain no right to enforce those duties.[164] Also, contrasted with Executive Orders, the informality of a memorandum to agency officials vitiates the policy's stability by making it simpler for later administrations to modify or ignore.[165]

The memorandum exemplifies an impetus to respond to criticisms of privacy protections, but builds upon the faulty foundation set by current privacy protections. The improvements collapse when confronted with the same objections raised against the foundation protections. This failure of patchwork policies to remedy invasions of privacy stresses the need for a structural solution.

Moreover, the 106th Congress flirted with privacy legislation.[166] Several bills proposed diverse methods to fill gaps in the current privacy protections.[167] Legislators expressed increasing concern about identity theft

---

163. *Compare* Privacy Memo, *supra* note 159, at Attachment A ("Protections afforded such information include the Privacy Act of 1974, the Computer Matching and Privacy Protection Act of 1988, the Paperwork Reduction Act of 1995, and the Principles for Providing and Using Personal Information . . . published by the Information Infrastructure Task Force on June 6, 1995 . . . ."), *with supra* Part I.B.2 (describing the problems with existing statutory protections).

164. Privacy Memo, *supra* note 159, at Attachment A ("This memorandum is intended only to improve the internal management of the executive branch and does not create any right or benefit, substantive or procedural, enforceable at law or equity . . . .").

165. President George W. Bush has shown no inclination to undo the effects of the Privacy Memo. In contrast, he has outlined a privacy plan based on the FTC's report on fair information practice principles—specifically notice, consent, access, and security. Michael J. Miller, *Bush's Privacy Plan*, PC MAGAZINE, Feb. 6, 2001, at 7, LEXIS, News Library, PC File ("I believe that privacy is a fundamental right, and that every American should have absolute control over his or her personal information." (quoting President Bush)); FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7-11 (July 1998). *But cf. supra* note 6 (describing Bush's efforts to further minimize the impact of the EU Data Privacy Directive even after the safe harbor provisions).

166. Declan McCullagh, *Pundits Speak*, HILL, Oct. 26, 2000 ("This was the first Congress that took privacy seriously. The legacy of the 106th Congress won't include aggressive privacy legislation - that'll happen next year - but it does include a growing distrust of . . . corporations' data collection practices . . . ."). *Contra* Dick Armey, *Privacy: For Those who Live in Glass Houses* (Apr. 9, 2001), *available at* http://www.freedom.gov/library/technology/memo/privacy.asp (expressing the concern of the House Majority Leader that privacy legislation should proceed slowly to avoid unintended consequences of hastily created laws).

167. *E.g.*, S. 2554, 106th Cong. (2000) (proposing to prohibit the public display of social security numbers for commercial purposes); S. 2699, 106th Cong. (2000) (proposing to regulate the sale and purchase of social security numbers); S. 2876, 106th Cong. (2000) (proposing massive amendments to the Social Security Act to enhance individual privacy); S. 3040, 106th Cong. (2000) (proposing the creation of a commission to study the appropriate balance of individual privacy and use of personal information); H.R. 220, 106th Cong. (1999) (proposing to eliminate government use of the social security number as an identifier and further proposing to prohibit any form of government-wide identification); H.R. 1450, 106th Cong. (1999) (proposing to regulate

and corporate sale of personal information and began focusing on data privacy regulations.[168] Although Congress did not pass any substantial social security number-related privacy bills, Congress opened the path for reform, and the proposed bills suggest the breadth of reform contemplated.

Forced to weigh government, business, and individual interests in personal information,[169] Congress struggles with the nascent wide-scale abuse of social security numbers in a global information era; the potential for abuse is only partially tapped by identity thieves and corporate marketing. The wide range in proposed legislative solutions, from superficial to structural, illustrate the possibility for significant improvement in individual privacy.[170] Considering the approaches and results of similarly situated countries will inform the debate and help establish an appropriate balance for U.S. players in the national and international setting.

II. National Identification Numbers in the United Kingdom and South Africa

As a basis for modifying U.S. privacy protections, this section examines three aspects of the United Kingdom and South Africa's approaches to national identification numbers: information management, privacy enforcement, and citizens' access to information. Information management refers to how the country compiles and disseminates information. A highly centralized approach collects individuals' information in a single location and allows other groups complete access to that information. A decentralized approach may isolate information in disparate locations or restrict access to collected information.

Privacy enforcement identifies how the country ensures compliance with existing privacy protections. A highly centralized approach empowers a single individual or agency with the sole responsibility of protecting citizens' privacy. A decentralized approach may leave citizens to seek enforce-

---

the sale of social security numbers and other marketing information without an individual's written consent); H.R. 3307, 106th Cong. (1999) (proposing that agencies conduct assessments of privacy implications resulting from proposed rulemaking); H.R. 3321, 106th Cong. (1999) (proposing that the FTC promulgate fair information practices to regulate the use of personal information).

168. *E.g.*, S. 2876, § 2 (expressing concern about fraud, identity theft, stalking, and privacy invasions from the exchange of social security numbers); H.R. 3321, § 2 (expressing concern about the compilation of personal information without an individual's knowledge); *Hearing on H.R. 220, the "Freedom and Privacy Restoration Act" Before the House Subcomm. on Gov't Mgmt, Info., & Tech. of the Comm. on Gov't Reform*, 106th Cong. (2000) (statement of Chairman Horn) [hereinafter *H.R. 220 Hearing*].

169. *H.R. 220 Hearing*, *supra* note 168 (statement of Barbara Bobvjerg, Associate Director of Education, Workforce, and Income Security Issues at the General Accounting Office) ("Congress must weigh such concerns about individual privacy . . . against the government's need for timely and accurate information to control payments and prevent fraud and abuse . . . . Moreover, limiting the use of SSN's in the commercial sector could slow or hamper some of the benefits of information sharing . . . .").

170. *Compare, e.g.*, H.R. 220 (advocating the removal of any vestige of national identification), *with* S. 2554 (prohibiting only the display of social security numbers for commercial purposes).

ment individually, split responsibility between several agencies, or force a single agency to handle several obligations in addition to citizens' privacy.

Citizens' access to information indicates how the country provides an individual access to his or her own information. A highly centralized approach allows the individual to compile all relevant sources and information in a single location. A decentralized approach forces the individual to locate agencies that maintain information on the citizen and contact each relevant agency to request information.

A. United Kingdom

In the United Kingdom, two defining historical moments set the tone for the national identification number debates. In 1951, the House of Lords struck down an incidence of "mission creep"[171] involving national registration identity cards issued for wartime security purposes.[172] In 1984, Parliament passed the Data Protection Act that established the Office of the Information Commissioner and conferred upon citizens a right to privacy in electronic records of personal information.[173] As a foundation for later privacy debates, these events emphasize relevant aspects of the United Kingdom's privacy approach.

1. *Information Management*

In December 1950, a police constable stopped Clarence Wilcock's automobile and demanded Wilcock's national registration identity card.[174] The National Registration Act required individuals to produce the cards when demanded by police.[175] Although enacted as an emergency measure after the outbreak of World War II, the statute did not contain a self-terminating clause.[176] Further, while created to maintain internal security, the police appropriated the registration numbers for other purposes, including index card files for drivers charged with criminal offenses.[177] When Wilcock refused to comply with the constable's request, the subtle expansion from

171. *Supra* notes 51-53 and accompanying text.

172. Wilcock v. Muckle, 2 K.B. 844 (1951).

173. Data Protection Act, 1984, ch. 35 (Eng.) (amended 1998). Parliament amended the Act in 1998 to conform protections to data privacy standards set by the European Union for member states. Info. Comm'r, *Preparing for the New Law - Data Protection Act 1998* (last modified July 1999), *at* http://www.dataprotection.gov.uk/prepare.htm; *see also* Data Privacy Directive, *supra* note 3.

174. *Wilcock*, 2 K.B. 844; *see also* Martin Bright, *Identity Cards: How the Cards Have Fallen*, GUARDIAN, May 30, 1995, 1995 WL 7606006 (providing more detail on Mr. Wilcock).

175. National Registration Act, 1939, 2 & 3 Geo. 6, ch. 91, § 6(4) (Eng.).

176. *Id.*; *see also Wilcock*, 2 K.B. 884 (debating the import of "emergency" in the statute and when the statute would effectively terminate).

177. *Id.* at 849 (testimony of Prosecutor Gattie in response to Lord Goddard's inquiry why police routinely requested identity cards for minor traffic violations). Other government agencies also appropriated the national registration number for unintended purposes. Bright, *supra* note 174 (describing uses by the War Office, the National Insurance Office, the Central Office of Information, the British Red Cross, and the British Empire Cancer Campaign).

an emergency statute to regular demands for identity documents left a lasting impression on the consciousness of the U.K. citizenry.

Responding to the reliance on the statute for routine situations, Lord Goddard remarked that police should respect the purpose for which the statute empowered officers to request identity cards.[178] After Goddard's admonishment, the government restricted information collection and distribution to the purposes for which the department needed the information.[179] As government record systems expanded beyond index card files and the efficiency value of identification numbers increased, the United Kingdom engaged in debates over national identity cards, but never adopted any national identification number.[180]

The resultant information management system used redundant databases and different identification numbers for each department. For national insurance, national health, and driver's licenses, individuals had distinct and unrelated identification numbers.[181] Although this inefficiency may be attributable to other factors,[182] each government department maintained information in databases that lacked a uniform standard conducive to data sharing.[183] This decentralized system of information

178. *Wilcock*, 2 K.B. 844 ("To use Acts of Parliament passed for particular purposes in wartime when the war is a thing of the past . . . tends to turn law-abiding subjects into lawbreakers, which is a most undesirable state of affairs.").

179. *E.g.*, Info. Comm'r, *Response by the Data Protection Registrar to the Modernising Government White Paper*, ¶¶ 13, 14 (May 1999) [hereinafter *Modernising Government Response*] (raising a concern that a proposed data sharing scheme would lead to use of information beyond the purpose for which it was obtained); *see also* Matthew Engel, *License to Snoop*, GUARDIAN, Aug. 22, 1994, 1994 WL 9295731 ("Twenty, ten, even five years ago, the idea of compulsory identity cards in Britain would have been unthinkable because everyone . . . was assumed to feel [that identity cards "will be used to bully, nanny and harass us by the police"] . . . after the police were attacked by Lord Chief Justice Goddard for abusing the system.").

180. *E.g.*, Green Net., *Mistaken Identity: Charter 88 Briefing on ID Cards* (last visited Feb. 12, 2000), *at* http://www.gn.apc.org/pmhp/dc/priv/idcards.htm (noting attempts to introduce national identity cards or numbers in the 1920s, 1978, 1988, 1989, 1990, 1992, 1993, and 1994); *see also* Valerie Elliott, *ID Smartcards Back on Agenda, Says Minister*, TIMES (London), Feb. 11, 1998, 1998 WL 4818334; Richard Ford, *Howard to Open ID Card Debate*, TIMES (London), Apr. 10, 1995, 1995 WL 7661231; Alan Travis, *Cabinet Shelves Identity Card Plan*, GUARDIAN, Oct. 14, 1996, 1996 WL 13381409; Keith Waterhouse, *Awkward Squad of Cards of Identity*, DAILY MAIL, May 24, 1999, 1999 WL 19061301; *cf.* Michael Cross, *What can HMG.org Offer Us?*, GUARDIAN, Mar. 25, 1999, 1999 WL 14125447 (noting that the national health number was issued with "the strict promise that no other agency would use it").

181. Cross, *supra* note 180 ("Different government departments use different identity numbers."); *ID Number for All in Scheme to Cut Fraud*, DAILY MAIL, July 3, 1999, 1999 WL 21588874 (noting "the complicated clutch of numbers held by Britons for national insurance, child benefit, the NHS and other purposes"); Waterhouse, *supra* note 180 (identifying the different identity cards, publicly and privately issued, that the author had in his wallet).

182. MODERNISING GOVERNMENT, 1999, Cmnd. 4310, ch. 1, ¶ 11.

183. *Id.* ch. 5, ¶ 4 ("[W]e have incompatible systems and services which are not integrated."); *Modernising Government Response*, *supra* note 179, ¶ 14 (noting the lack of "common data standards across the public sector"); *see also* Cross, *supra* note 180 ("All [government departments] have their own ways of handling information; [they] even hold names and addresses in different incompatible formats.").

management minimized any of the theoretical risks from national identification numbers in networked databases because the United Kingdom's databases could not be linked effectively.[184]

2. *Privacy Enforcement*

Even if departments shared information with other public or private entities, the United Kingdom provided privacy protection through the Data Protection Act, which created the Office of the Information Commissioner (Commissioner).[185] The Commissioner operates independently from other agencies and reports directly to Parliament.[186] The Data Protection Act authorizes the Commissioner to maintain a list of organizations that collect and use personal data,[187] disseminate information about the Data Protection Act,[188] promote and assist compliance with the Data Protection Principles,[189] process complaints, and prosecute violations.[190]

---

184. *Supra* Part I.A (identifying the dangers of using national identification numbers with networked databases); *see also* MODERNISING GOVERNMENT, *supra* note 182, ch. 5, ¶ 4 ("Government has so far followed a largely decentralised approach to IT development."). The government has taken steps to change the existing system by formulating data standards and linking department databases to remove inefficient redundancies. MODERNISING GOVERNMENT, *supra* note 182; *see also* Cross, *supra* note 180 ("The [Modernising Government] white paper will propose linking agencies' information systems on a colossal national intranet, which could have up to 600,000 users."). Also, the United Kingdom has started to contemplate using nonidentification smart cards. INFO. AGE GOV'T CHAMPIONS, FRAMEWORK FOR INFORMATION AGE GOVERNMENT: SMART CARDS (Apr. 2000), *available at* http://www.e-envoy.gov.uk/egovernment/iagc/pdfs/Smartcards.pdf; BBC News, *Bracknell Forest Goes Virtual* (Jan. 24, 2001), *at* http://news.bbc.co.uk/hi/english/sci/tech/newsid_1134000/1134559.stm.

185. *E.g.*, David Brindle, *Data Registrar Warns NHS*, GUARDIAN, Apr. 15, 1993, 1993 WL 9906897 (recounting the Information Commissioner's response to complaints that hospitals and health authorities may be sharing unnecessary and detailed personal information). *See generally* Info. Comm'r, *A Guide to Developing Data Protection Codes of Practice on Data Matching* (July 1997), *at* http://www.dataprotection.gov.uk/match.htm (setting guidelines to insure that public and private sector data matching programs comply with the Data Protection Principles). Unlike the Privacy Act in the United States, the Data Protection Act subjects public and private organizations to regulations for use of personal information. *Compare* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552(f)(1) (1999)), *and supra* notes 112-13 and accompanying text, *with* Data Protection Act, 1998, ch. 29, pt. 1, § 1 (Eng.) (defining data controllers and data processors as anyone that collects, uses, or discloses personal information).

186. Data Protection Act, 1998, ch. 29, pt. 1, § 6, sched. 5, pt. 1, § 1(2); Info. Comm'r, *Data Protection Summary* (last modified Nov. 1999), *at* http://www.dataprotection.gov.uk/summary.htm.

187. Data Protection Act, 1998, ch. 29, pt. 3, § 19; Info. Comm'r, *The Data Protection Register: Search Form* (last visited Apr. 25, 2001), http://www.dpr.gov.uk/search.html (allowing individuals to search the list of registered data collectors).

188. Data Protection Act, 1998, ch. 29, § 51.

189. 1. Personal data shall be processed fairly and lawfully . . .
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.

With the ultimate responsibility to protect individuals' privacy, the Commissioner functions as an independent centralized gateway for any use of personal information.[191] The Commissioner's independence and singular purpose to protect privacy ensure an effective check on efforts by the public and private sector to abuse shared databases.[192] The Commissioner analyzes the privacy implications of proposed data usage without the necessity of weighing other factors. Furthermore, unlike the Privacy Act's remedy provisions, the Commissioner's powers of registration and enforcement impose proactively uniform regulation.[193] Where U.S. citizens must individually file suit to protect their privacy rights, the Commissioner processes complaints from U.K. citizens and pursues violations on their behalf.

3. *Citizens' Access to Information*

The Data Protection Act also conveyed citizen-initiated rights,[194] including access to personal information.[195] The right to access functions in a manner similar to the Privacy Act protections.[196] Individuals may request personal information stored by government or corporate organizations, and the Data Protection Act sets procedures for the organization's response, including regulations for honoring their requests for correction or deletion

---

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Id. sched. 1, pt. 1.

190. *Id.* ch. 29, pt. 5, §§ 40-50.

191. Although the OMB features prominently in the Privacy Act and the Privacy Memo as a similar protector, one commentator argues forcefully that the OMB's role considers privacy only as a small factor in balances of efficiency and cost. *Compare* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a(v) (1999)), *and* Privacy Memo, *supra* note 159, at Attachment A, *with* Schwartz, *supra* note 70, at 602. President Clinton did appoint a Chief Counselor for Privacy as part of the OMB to advise the President on policy decisions, but the position did not entail any enforcement power similar to the Commissioner. Elizabeth Weise, *Privacy is Peter Swire's Domain*, USA TODAY, June 7, 2000, LEXIS, News Library, USATDY File.

192. *E.g.*, Info. Comm'r, *Response of the Data Protection Registrar to the Government's Proposals for Identity Cards* (Sept. 1996), *at* http://www.dataprotection.gov.uk/idcm3362.htm (criticizing proposed photo driver's license).

193. *Compare* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1897 (codified as amended at 5 U.S.C. § 552a(g) (1999)), *and supra* notes 112-14 and accompanying text, *with* Data Protection Act, 1998, ch. 29, §§ 40-50, *and* Info. Comm'r, *Enforcement Statement* (June 1999), *at* http://www.dataprotection.gov.uk/enforce.htm.

194. Data Protection Act, 1998, ch. 29, §§ 7-15.

195. *Id.* § 7.

196. *Compare id.*, *with* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1897 (codified as amended at 5 U.S.C. § 552a(d) (1999)).

of records.[197] Through the list of registered organizations that use and collect data, the Data Protection Act provides citizens a centralized database of locations for citizens' personal information and descriptions of the information stored.[198] This directory facilitates efforts to limit distribution of personal information and ensure the accuracy of data used. Yet, citizens must contact organizations individually.[199]

This sketch of the United Kingdom's approach to data privacy may be summarized according to the three aspects. Although evolving,[200] the government's information management functions as a decentralized system of mostly incompatible databases.[201] Privacy enforcement rests with a centralized independent government official whose sole purpose involves protection of data privacy.[202] Finally, for disclosure of personal information, citizens have centralized access to data locations, but decentralized access to the information.[203]

B. South Africa

In contrast to the United Kingdom, South Africa has used identity documents, including national identification numbers, since at least 1986.[204] Accordingly, South Africa's citizens retain a relative comfort with national identification numbers.[205] Yet, an interesting aspect of South Africa's gov-

197. Data Protection Act, 1998, ch. 29, §§ 7-15.
198. *Id.* §§ 16-19; Info. Comm'r, *supra* note 187.
199. Data Protection Act, 1998, ch. 29, § 7(2)(a).
200. *Supra* note 184.
201. *Supra* notes 181-84 and accompanying text.
202. *Supra* notes 185-93 and accompanying text.
203. *Supra* notes 195-99 and accompanying text.
204. §§ 5, 8 of Identification Act No. 72 of 1986 (BSRSA). During the apartheid era prior to 1986, the government required black citizens to carry identity documents referred to as "dompas." Patrick Laurence, *A Question of Mathematics*, FIN. MAIL, Sept. 18, 1998, at 40.
205. *E.g.*, Stephen Mulholland, *Say Thanks to Those Trying to Ensure a Fair Election*, BUS. TIMES, Jan. 10, 1999, at 1 ("[Government officials] are capturing the data that will assist the growth of a modern state in SA, a state in which, without playing Big Brother, the authorities can locate and account for each member of society."); *'Smart Cards' Illogical, Says DP*, SOUTH AFRICAN PRESS ASS'N, Feb. 1, 2000, 2000 WL 4006574 ("Despite the long queues, bureaucratic bungling and inconvenience, the vast majority of citizens responded positively and made the effort to apply for bar-coded IDs."); Dispatch Online, *Editorial Opinion: Question of Identity* (Sept. 17, 1997), *at* http://www.dispatch.co.za/1997/09/17/page%2010.htm ("The most important single exercise in good government presently under way in South Africa is almost without question the installation of the Home Affairs national identification system . . . ."); *cf.* David Shapshak, *SA Services Get 'Smart,'* MAIL & GUARDIAN, Apr. 24, 1998, 1998 WL 10888992 (identifying numerous beneficial uses for smart cards, but noting potential concerns of government tracking or invasions of data privacy raised by a British author). *Contra* DEP'T OF COMMUNICATIONS, A GREEN PAPER ON ELECTRONIC COMMERCE FOR SOUTH AFRICA 66-74 (Nov. 2000), *available at* http://www.ecomm-debate.co.za/greenpaper/greenpaper.pdf; Dep't of Communications, *Discussion Paper on Electronic Commerce*, § 4.2 (July 1999), *available at* http://www.ecomm-debate.co.za/docs/discuss04.html (raising concerns regarding data sharing and use of personal information); Pamela Whitby, *How to Put Big Brother on a Smart Leash*, BUS. DAY, Sept. 9, 1999, at E8 (arguing that pending privacy legislation should be accelerated prior to implementing new identity technology).

ernment is the recent significant revision of its written constitution.[206] As a consequence of the constitution's infancy, the additional rights and procedures conferred do not correlate to well-established doctrine, making it difficult to evaluate any stated privacy protections.[207] However, the government's plans for identity documents provide an informative structural model to contrast with the United Kingdom, even if the final system develops differently.

1. Information Management

Dating to the passage of the constitution's final draft, the government circulated plans for a new national identification system implemented by the Department of Home Affairs.[208] Over the intervening years, the method and purpose of the identification system expanded. Originally conceived as the ultimate document for identity verification, the first tender[209] described a card using individuals' photographs and fingerprints.[210] Without discarding the verification purpose and protections, the final tender encompassed a more ambitious effort[211] to unify citizens' personal infor-

206. S. AFR. CONST. 1996; *see also* S. AFR. CONST. (Interim Constitution, 1993).

207. *E.g.*, Mistry v. Interim Nat'l Med. and Dental Council of S. Afr., 1998 (7) BCLR 880 (CC) (ruling that the constitution's right to privacy clause, S. AFR. CONST. § 13, does not explicitly protect informational privacy, *supra* Part I.B.2.a.ii, but refusing to discuss whether informational privacy falls implicitly within the ambit of the constitution because the case could be otherwise disposed); *cf.* Barry Streek, *New Bills Promote Transparency*, MAIL & GUARDIAN, Jan. 28, 2000, 2000 WL 4131480 (arguing that it would take years for lawyers and bureaucrats to define the scope and effect of South Africa's version of the Freedom of Information Act). *Compare* Promotion of Access to Information Act 2 of 2000 (BSRSA), *with* Freedom of Information Act of 1966, Pub. L. No. 89-487, 80 Stat. 250 (codified as amended at 5 U.S.C. § 552 (1999)).

208. Dep't of Home Affairs, *Launching a New Identification System* (July 29, 1996), *available at* http://www.polity.org.za/govdocs/pr/1996/pr0729.html; *see also* S. AFR. CONST. of 1996 (adopted May 8, 1996 and amended Oct. 11, 1996 to conform to certification objections leveled by the Constitutional Court, 1996 (10) BCLR 1253 (CC)).

209. "A formal offer, as: . . . a written offer to contract goods or services at a specified cost or rate; a bid." AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (3d ed. 1996).

210. Mangosuthu G. Buthelezi, Minister of Home Affairs, Introductory Speech: Budget Debate before the National Assembly (Apr. 17, 1997) (transcript available at Southern African Migration Project, *at* http://www.queensu.ca/samp/migdocs/speech1.htm) (detailing the purposes of the card to "restrict persons to a single, unique identity number" for public and private records and "ensure that the person is who he/she claims to be," and describing the identity verification elements as a link to an existing, centralized database of personal information, a link to a fingerprint database of citizens' thumbs, and the presentation of a valid identification card); *see also* Dep't of Home Affairs, *supra* note 208 (detailing the identity verification procedures as "visual inspection of the card, person and photograph, stand-alone verification, which reads the stored information on the card and on-line verification, which will allow the person and card to be compared to the information stored on the central database").

211. Pamela Whit, *National Identity System Faces Technical Challenges*, BUS. DAY, Dec. 7, 1999, 1999 WL 25958756 [hereinafter Whit, *National Identity System*] (noting that the proposed identification system would be the largest "civilian automated fingerprint identification system . . . in the world"); Pamela Whit, *Smart-card Decision Causes Consternation in Industry Circles*, BUS. DAY, Aug. 23, 1999, 1999 WL 22792247 [hereinafter Whit, *Smart-card Decision*] (remarking that the smart card proposal would be a "massive

mation on smart cards.[212]

Due to the lack of technological infrastructure, the smart cards presented a cost-effective solution for providing government services and benefits.[213] Government officials in remote regions would not need connections to networked databases because identity verification and relevant information about a citizen could be accessed using an independent smart card reader.[214] To maintain the integrity of the information, the smart cards would be synchronized with an extensive database that contained essential information about the citizen, including fingerprints.[215] The Director-General of the Department of Home Affairs would retain complete control over the information stored in the centralized database.[216]

The government expects that the smart card will be used by both public and private entities with the centralized database compiling an entire file of the individual's personal information.[217] Possible applications for the smart card include uses in "housing, schools, hospitals, and even jobs" with vital information ranging from birth and marriage to financial and medical.[218] One common example of the potential for cross-over uses between the public and private sectors involves collection of pension benefits.[219] As conceived, a citizen could synchronize the smart card with a government database to download that citizen's benefits on to the smart

---

and expensive undertaking, but could be a world first" due to the scope of the uses proposed).

212. Shapshak, *supra* note 205 (detailing potential storage of information for driver's license, bank accounts, health records, and security clearances); Whit, *Smart-card Decision*, *supra* note 211 (stating that government officials for "health, welfare, labour[,] housing, justice, the SA Police Service and the State Information Technology Agency" were interested in uses for the smart card).

213. Whit, *Smart-card Decision*, *supra* note 211 ("Since smart cards can operate offline, they have the ability to overcome some of the barriers . . . such as the lack of infrastructure in SA's rural areas.").

214. *Id.*; Whitby, *supra* note 205 ("All a government official would require is a smart card reader.").

215. *Supra* note 208; *see also* §§ 8, 14 of Identification Act 68 of 1997 (BSRSA).

216. §§ 6, 21 of Identification Act 68 of 1997; *see also* Mangosuthu G. Buthelezi, Minister of Home Affairs, Media Briefing (Sept. 10, 1997) (transcript available at Unwembi's Resource of South African Government Information, *at* http://www.polity.org.za/govdocs/speeches/1997/sp0910.html) (describing the Identification Act of 1997 as allowing the Minister to permit "restricted access to the Population Register . . . at the same time ensuring that the privacy of individuals . . . is being protected").

217. Mangosuthu G. Buthelezi, Minister of Home Affairs, Media Briefing (Aug. 31, 1999) (transcript available at Unwembi's Resource of South African Government Information, *at* http://www.polity.org.za/govdocs/speeches/1999/sp0831b.html) (noting considerations to "provide [South Africa's] citizens with a more versatile form of identification, which they can use in their dealings with other organs of the state, and even for private uses"). On a much more local scale, communities in the United Kingdom are currently considering smart cards for interactive government services. BBC News, *supra* note 184.

218. Dispatch Online, *Editorial Opinion: Hanis, Afis, Saps & Sars* (Feb. 16, 2001), *at* http://www.dispatch.co.za/2001/02/16/editoria/aleader.htm; *see also* Dispatch Online, *Cabinet Yes for Smart Card Expected Soon* (Feb. 13, 2001), *at* http://www.dispatch.co.za/2001/02/13/southafrica/parlysma.htm.

219. *E.g.*, Shapshak, *supra* note 205.

card.[220] Once downloaded, the citizen could use the smart card as a debit or ATM card to purchase goods or withdraw money.[221] So characterized, South Africa's smart card presents a form of highly centralized information management.[222]

2. *Privacy Enforcement*

With a strongly centralized form of information management, an equally strong form of privacy protection would mitigate the danger of disclosing unnecessary personal information. South Africa, however, splinters privacy enforcement responsibility into four groups: the individual citizen, Director-General of Home Affairs, Human Rights Commission, and Public Protector. In general, individual citizens act for the single purpose of protecting their privacy and may seek enforcement in the courts.[223]

In contrast, each government organization with responsibility for citizens' privacy only weighs the obligation as a minor factor in the balance of the agency's primary duty. The Director-General of Home Affairs' duty to implement the national identification system and Population Register entails consideration of citizens' privacy in the information collected.[224] Given the Department of Home Affairs' explicit open-ended discretion and the continuing expansion of potential uses for the smart card, however, the Director-General displays little commitment to data privacy.[225]

The Human Rights Commission functions as the protector of fundamental rights enumerated in the constitution.[226] Within those duties, the Human Rights Commission has the authority to pursue violations of privacy and human dignity, but also has the responsibility to monitor infringements of divergent concerns such as access to courts, political rights, education, and social security.[227] Consequently, even if the constitution explicitly recognized a right to data privacy,[228] the Human Rights Commission could not and does not devote significant resources to protecting citizens' privacy.[229]

---

220. *Id.* (describing a system of government kiosks that provide services and government information keyed to the smart card, such as pension benefits); *supra* note 210 (noting links to a centralized database).

221. *E.g.*, Buthelezi, *supra* note 217.

222. Whit, *National Identity System*, *supra* note 211 ("'Instead of each department issuing a separate card there will now be one multipurpose card and one infrastructure . . .' says [Home Affairs Chief Director of Information Technology, Patrick] Monyeki.").

223. *E.g.*, Mistry v. Interim Nat'l Med. and Dental Council of S. Afr., 1998 (7) BCLR 880 (CC) (describing an individual seeking protection under the constitutional right to privacy).

224. *Supra* note 216 and accompanying text.

225. *Supra* notes 212, 216-18 and accompanying text.

226. South African Human Rights Comm., *SAHRC - Profile* (last visited Feb. 13, 2000), *at* http://www.sahrc.org.za/sahrc/profile/profile.html; *see also* S. AFR. CONST. ch. 2.

227. S. AFR. CONST. ch. 2.

228. *Supra* note 207.

229. South African Human Rights Comm., *SAHRC - Standing Committees* (last visited Feb. 13, 2000), *at* http://www.sahrc.org.za/sahrc/committees/committees.html

The Public Protector acts as an independent investigator for complaints against government officials.[230] While this mandate could include allegations of privacy violations, the Public Protector focuses on complaints of government corruption, wasteful administration, and improper conduct.[231] Therefore, South Africa applies a decentralized system of privacy enforcement, splintering responsibility for privacy protections among several agencies that have other significant obligations.

3. *Citizens' Access to Information*

After slight examination, the smart card epitomizes the ideal for centralized citizen access to information. Using the smart card to compile personal information, the citizen will always carry a copy of any relevant government and corporate information.[232] However, centralized access requires that the citizen retains the rights to read the information stored on the smart card and correct or dispute any erroneous information.[233]

The preliminary groundwork for these rights rests on the Promotion of Access to Information Act (Information Act).[234] The Information Act permits citizens to request information from public and private organizations.[235] If the citizen complies with procedural requirements, their right to access government databases extends to all information held in the databases—subject to specific exceptions, including exemptions to protect third-party privacy or confidentiality, public safety and national security, and economic stability.[236] For access to private databases, the citizen must seek the information in furtherance of the exercise or protection of the citizen's rights, subject to exceptions similar to those affecting access to government information.[237] The additional requirement for private databases, however, does not hinder citizens' access because personal data qualifies explicitly as information necessary for the furtherance of the citi-

---

(describing the purpose and scope of the Commission's standing committees); South African Human Rights Comm., *SAHRC - Projects* (last visited Feb. 13, 2000), *at* http://www.sahrc.org.za/sahrc/projects/projects.html (reporting on the purpose and progress of the Commission's existing projects); *see also* Streek, *supra* note 207 (explaining the role of the Human Rights Commission in enforcing the Promotion of Access to Information Act, §§ 83-85 of Promotion of Access to Information Act 2 of 2000 (BSRSA), and noting the funding and resource difficulties that could hinder the Commission's compliance).

230. Office of the Public Protector, *The Public Protector* (last visited Feb. 13, 2000), *at* http://www.polity.org.za/govt/pubprot/pubprot.html.

231. *Id.*

232. *Supra* notes 212, 217-18 and accompanying text.

233. *See* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a(d) (1999)); Data Protection Act, 1998, ch. 29, §§ 7, 14 (Eng.); *cf.* Schwartz, *supra* note 70, at 595 ("The critical individual rights concern access to personal records and the opportunity to request their amendment.").

234. §§ 11-73, 88 of Promotion of Access to Information Act 2 of 2000 (BSRSA) (enacted to execute the constitutional right to access, S. AFR. CONST. ch. 2, § 32; Preamble of Promotion of Access to Information Act 2 of 2000).

235. *Id.*

236. *Id.* §§ 11-49.

237. *Id.* §§ 50-73.

zen's rights.[238] The Information Act effectively combines and expands the rights to access conferred on U.S. citizens by the Freedom of Information Act and Privacy Act.[239]

Even with access to information, citizens must be able to correct erroneous data.[240] The Information Act takes a preliminary step by requiring that government and private entities process citizens' requests for corrections of information.[241] However, the Information Act only commands organizations to institute an internal process for handling corrections as a interim measure until Parliament enacts legislation providing citizens specific procedural rights.[242] With these rights, South Africa's citizens could easily use the smart card to download, browse, and correct personal information maintained on government and private databases.[243] This potential approach presents a highly centralized form of citizens' access to information.

III. Method for Formulating a Structural Solution: Definitions and Premises

As privacy debates flare in response to new technology,[244] two premises should be established: (1) substantial changes in the distribution of information require structural modifications to information control and (2) as

238. *Id.* § 50(3); *cf. id.* § 1 (defining personal information).

239. *Compare id.* (granting access to government and privately held personal information), *with* Freedom of Information Act of 1966, Pub. L. No. 89-487, 80 Stat. 250 (codified as amended at 5 U.S.C. § 552 (1999)) (government-held information), *and* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1897 (codified as amended at 5 U.S.C. § 552a(d) (1999)) (government-held personal information).

240. *E.g.*, *supra* note 197 and accompanying text.

241. § 88 of Protection of Access to Information Act 2 of 2000.

242. *Id.*

243. *Id.* §§ 18, 29, 53 (allowing electronic submission of requests for access and permitting access in electronic form or as otherwise requested by the citizen); *see also* Shapshak, *supra* note 205 (describing government kiosks for downloading information); Whitby, *supra* note 205 (noting the existence of portable smart card readers for browsing information). While the Information Act prescribes a set form for information requests, the smart card could be programmed to properly configure a citizen's request and automatically submit the request electronically upon completion. The European Commission recently subsidized research into technology to protect individual privacy during electronic requests for information. Press Release, Privacy Incorporate Software Agent, Fast and Safe Internet Work with PISA (Jan. 17, 2001), *available at* http://www.tno.nl/instit/fel/pisa/press_release_start_pisa_17012001.html.

244. *E.g.*, Robert Lemos, ZDNet, *Rights Groups Call for ID Tracking Laws* (Mar. 9, 1999), *at* http://www.zdnet.com/pcweek/stories/news/0,4153,2222299,00.html (recounting privacy debate over Microsoft's collection of information during online registration despite lack of consumer consent and Intel's use of computer chips that silently broadcast individualized identification numbers over the Internet); Courtney Macavinta, CNET, *Privacy Fears Raised by DoubleClick Database Plans* (Jan. 25, 2000), *at* http://news.cnet.com/news/0-1005-200-1531929.html (discussing privacy concerns provoked by the merger of online advertiser, DoubleClick, with catalog merchant, Abacus Alliance); ZDNet, *RealNetworks is Watching You* (Nov. 1, 1999), *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2385034,00.html?chkptzdnntop (recounting privacy debate over background collection of music downloaded from the Internet using company's software).

technology creates problems, technology holds the means to solving those problems. An explanation of these premises provides perspective for understanding the nature of the solution this Note seeks. With the proper perspective, analysis of the United Kingdom and South Africa models provides principles upon which to base a solution for the United States.

A. Rights vs. Structure

The first premise acknowledges the way technology pervades our society.[245] Convenience for consumers, businesses, and government agencies contributes to the expansion of increasingly invasive technology into all aspects of everyday life.[246] For example, as society moves from cash to electronic payments, such as credit cards, a purchase trail materializes that does not rely on receipts or human memory.[247] Did Barry uses his credit card to purchase something from Texaco two months ago for five dollars? Most likely, Barry discarded any paper receipt of the purchase and does not remember details. On the other hand, the credit card company recorded the seller's name, location, date, time, and amount of the purchase.[248] Theoretically, this information could be stored indefinitely.[249]

The credit card company's collection serves legitimate goals of administrative efficiency,[250] consumer protection, and liability avoidance. Storing the information enables the company to comply efficiently with a Fair Credit Billing Act provision governing prompt response to billing disputes[251] and a Truth in Lending section limiting cardholder liability to fifty dollars for fraudulent use of the card.[252] Thus, the cardholder benefits from the consumer protection provisions and efficient service.

The lure of convenience, however, ingratiates technology into daily life. The need for advanced services permits the slow erosion of mundane anonymity.[253] In many facets of modern life, such as grocery purchases and home telephone calls, activities once believed private only because considered trivial or insignificant are tracked and stored by the firms providing the underlying service.[254] In many cases, individuals must tolerate

245. *E.g.*, Grossman, *supra* note 14, at 1010-13.
246. *Supra* notes 13, 15 and accompanying text.
247. Swire, *supra* note 13, at 464-67.
248. *Id.* at 465.
249. Although current storage media, such as computer hard drives, only last about ten years, the capability of transferring data to new media means data could be stored indefinitely. *See generally* M. Halem et al., Earth & Space Data Computing Division, NASA, *Technology Assessment of High Capacity Data Storage Systems: Can We Avoid a Data Survivability Crisis?* (Feb. 2, 1999), *at* http://sdcd.gsfc.nasa.gov/ESDCD/whitepaper.data_survive.html (describing the need for a policy to maintain constant data migration to new media to preserve indefinitely the mass of historical documents stored on aging media).
250. *Supra* note 13 and accompanying text.
251. Pub. L. No. 93-495 (1974) (codified as amended at 15 U.S.C. § 1666 (1999)).
252. Pub. L. No. 91-508, 84 Stat. 1126 (1970) (codified as amended at 15 U.S.C. § 1643(a)(1)(B) (1999)).
253. Swire, *supra* note 13, at 464.
254. *Id.*

this invasive collection of information or forego the service,[255] leading some to conclude that an expectation of privacy is the sacrificial lamb of modernization.[256]

1. Rights-Based Privacy

The struggle between privacy and technology arises from a failure of traditional notions of rights-based privacy to recognize the structural inequity formed in an era where a single piece of information represents power beyond that revealed by examining the information in isolation.[257] In general, the U.S. government grants individuals rights for the purpose of promoting individual autonomy and empowering them as active participants in society.[258] The United States protects freedom of speech, prohibits unauthorized searches, and bars cruel and unusual punishment in part to encourage citizens by leveling inequitable power distribution between individuals and government agencies or corporate firms.[259] For example, the

255. *Supra* notes 53-56, 154 and accompanying text.

256. Grossman, *supra* note 14, at 1013; CONSUMER PRIVACY SURVEY, *supra* note 14, at 70.

257. *Compare supra* Part I.B.2.a.ii, b.ii (describing the rise of U.S. informational privacy and subsequent failure of courts to uniformly protect individuals against government disclosure or use of social security numbers capable of revealing detailed personal information), *with* Doe v. Registrar of Motor Vehicles, No. 85-3449, 1993 Mass. Super. LEXIS 286, at *11-24 (Mass. Super. Ct. June 8, 1993) (recognizing the aggregating power of information, but declining to apply a right to privacy to restrict access to any information, including social security numbers), *with supra* Part I.A (noting the intrinsic risk in networked databases of enabling detailed retrieval of personal data when an individual only discloses a national identification number or trivial personal information).

258. The constitutional right of free expression is . . . designed and intended to remove governmental restraints from the arena of public discussion, putting the decision as to what views shall be voiced largely into the hands of each of us, in the hope that use of such freedom will ultimately produce a more capable citizenry and more perfect polity and in the belief that no other approach would comport with the premise of individual dignity and choice upon which our political system rests.

Cohen v. California, 403 U.S. 15, 24 (1971); *see also* 1 JOURNALS OF THE CONTINENTAL CONGRESS 108 (Worthington C. Ford et al. eds., 1774) ("The importance of [freedom of the press] consists . . . in its diffusion of liberal sentiments on the administration of Government, its ready communication of thoughts between subjects, and its consequential promotion of union among them, whereby oppressive officers are shamed or intimidated, into more honourable and just modes of conducting affairs."), *quoted in* Roth v. United States, 354 U.S. 476, 484 (1957). It is beyond the scope of this Note to discuss the possibility of conflicts between rights, such as between free speech and privacy. *E.g.*, Bartnicki v. Vopper, 200 F.3d 109 (3d Cir. 1999), *cert. granted*, 68 U.S.L.W. 3789 (U.S. June 26, 2000) (No. 99-1687); SOLEVIG SINGLETON, PRIVACY AS CENSORSHIP: A SKEPTICAL VIEW OF PROPOSALS TO REGULATE PRIVACY IN THE PRIVATE SECTOR (Cato Inst., Policy Analysis No. 295, 1998); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000). Regulation of collected personal data may not, however, implicate First Amendment concerns. *E.g.*, Trans Union Corp. v. FTC, No. 00-1141, 2001 U.S. App. LEXIS 6241 (D.C. Cir. Apr. 13, 2001) (denying a First Amendment claim asserted for personal information that the FTC claimed was subject to the Fair Credit Reporting Act—imposing privacy regulations on consumer reporting agencies).

259. *E.g.*, JOHN LOCKE, CONCERNING CIVIL GOVERNMENT: AN ESSAY THE TRUE ORIGINAL EXTENT AND END OF CIVIL GOVERNMENT (Robert Maynard Hutchings et al. eds., 1952)

right to equal protection of the laws empowered African-American citizens to expand their participation in society through the diverse aspects of the Civil Rights Movement, including the integration of schools and increased involvement in national political debate.[260]

While the rights-based model of governance laudably equalizes citizens, the privacy right's scope has stagnated in the United States.[261] The Supreme Court justified this stagnation by explaining that "the guideposts for responsible decisionmaking in this unchartered area are scarce and open-ended."[262] This response begs the question because the Court formulated the original categories of fundamental rights without explicit guidance.[263] Accordingly, the Court's justification only hinders the progress of fundamental rights analysis at an arbitrary and incomplete stage of development. This stagnation may arguably be justified, however, under the assumption that citizens retain sufficient protections to secure their individual autonomy.[264]

Yet, a rights-based model cannot remain stagnant during a period of rapid technological advancement. In the last forty years, the power of information has increased exponentially. Previously, information only wielded power if sufficiently intimate or personal. For example, in the 1960s, the average person with a only a phone number could not use that information for any purpose other than to call the individual to whom the number belonged. Now, the same person with only a phone number could retrieve a name and address with minimal effort over the Internet.[265] With the name, address, and phone number, the person holds sufficient information to retrieve further data from government agencies, such as public

(1690) (describing the power inequities between the government and individuals caused by citizens' relinquishing power upon entering society for the benefit of the government's protecting the citizens' life, liberty, and property); *see also* Shapiro, *supra* note 34 (noting the unequal bargaining position of individuals and marketing companies as a problem with self-regulation). Locke's essays influenced the framing of the U.S. Constitution. United States v. Ganz, 806 F. Supp. 1567, 1575 (S.D. Fla. 1992) ("The consent theory of government, expounded by philosophers such as John Locke . . . and adopted by our founding fathers, supports the concept of a government entrusted by the people with carrying on the affairs common to us all."); Encyclopædia Britannica, *John Locke: Political Theory* (last visited Feb. 18, 2000), *at* http://www.britannica.com/bcom/eb/article/1/0,5716,114881+12+108465,00.html ("Locke formulated the classic expression of liberalism, which was to inspire both the shapers of the American Revolution and the authors of the U.S. Constitution.").

260. WINI BREINES, COMMUNITY AND ORGANIZATION IN THE NEW LEFT: 1962-1968 21-23 (1982).

261. Collins v. City of Harker Heights, Tex., 503 U.S. 115, 125 (1992) (expressing a reluctance to expand the categories of fundamental substantive rights); *see also supra* note 130 and accompanying text.

262. *Collins*, 503 U.S. at 125.

263. *E.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) (articulating a right to privacy from implicit principles in the Constitution and cultural history); *see also supra* notes 91-94 and accompanying text.

264. *E.g.*, Bibas, *supra* note 23 (advocating contractual solutions to privacy concerns).

265. *Supra* note 22 (discussing reverse search technology).

records and criminal history.[266] Therefore, with each piece of information provided to the government or private firms, the individual yields significant power to that entity.[267] This dangerous redistribution of power poses a greater threat as organizations realize the rights-based model does not respect a strong right to information control, prompting collection of information without the informed consent of citizens.[268]

Unfortunately, the risk in stressing the power of information is a backlash against information collection and data services. Yet often, as the example with Barry's credit card illustrates, the collection and dissemination of information is not necessarily malicious.[269] Progress entails information exchange and storage as citizens seek services and must relinquish personal information,[270] but it does not necessitate a lessened expectation of privacy.[271] The judiciary, however, has not been able to formulate a

266. *E.g.*, *Living in the Global Goldfish Bowl*, ECONOMIST, Dec. 18, 1999, LEXIS, News Library, ECON File (following the efforts of a private investigator and "blagger"—a person that collects minimal personal information about another individual then poses as that person—to obtain more detailed information about the author).

267. *E.g.*, United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 765 (1989) ("[T]hese statutes and regulations . . . evidence a congressional . . . recognition of the power of compilations to affect personal privacy that outstrips the combined power of the bits of information contained within.").

268. *E.g.*, Ed Bott, *How Progress Killed Privacy*, SMART BUSINESS, Mar. 2000, *available at* http://www.zdnet.com/smartbusinessmag/stories/all/0,6605,2429470-2,00.html ("The incentives just aren't there for the industry to provide meaningful privacy rights to consumers." (quoting David Sobel, General Counsel, Electronic Privacy Information Center)); Sovern, *supra* note 16, at 1074-90 ("As a result, as long as marketers have the power and incentive to inflate strategic transaction costs, the market is unlikely to produce an efficient equilibrium.") (describing the methods and motivation of businesses to make it difficult for consumers to protect personal information); *see also* Junkbusters, *How Web Servers' Cookies Threaten Your Privacy* (last visited Feb. 18, 2000), *at* http://www.junkbusters.com/ht/en/cookies.html (describing the information collected without an individual's knowledge when Internet servers use cookies and setting steps to disable the cookies functionality, which allows people to assert their right to privacy but at the cost of cookies' convenience); *Michigan Attorney General Granholm Files Action Against DoubleClick Over Privacy Issues*, PR NEWSWIRE, Feb. 17, 2000. Westlaw, ALLNEWSPLUS File (reporting that the Michigan Attorney General initiated legal action against Doubleclick for using Internet cookies to track consumers' personal information without consent). The reality of these concerns has manifested during bankruptcy proceedings of Internet companies that sought to sell databases of personal information collected from users. Heather Green, *Your Right to Privacy: Going . . . Going . . .*, Bus. Wk., Apr. 23, 2001, at 48, LEXIS, News Library, BUSWK File (describing the bankruptcy efforts of Toysmart.com and Voter.com to sell databases of 250,000 and 170,000 users respectively and explaining that many companies are unilaterally changing their privacy policies for consumer information to avoid FTC scrutiny of similar sales) ("[C]ustomers can do little to stop [online companies] from selling information thought to be confidential."); *cf.* Press Release, TRUSTe, TRUSTe Seeks Public Comment on Privacy Guidelines for Companies Undergoing Mergers, Acquisitions and Bankruptcies (Apr. 11, 2001), *available at* http://www.truste.org/about/about_mabs.html (proposing self-regulation guidelines for corporate transfer of personal information databases in bankruptcy contexts).

269. *Supra* notes 247-52 and accompanying text.

270. Schwartz, *supra* note 18, at 1332-34; *see also* Grossman, *supra* note 14, at 1013.

271. *Infra* Part IV.A.3 (balancing interests in privacy and convenience to formulate a structural solution to privacy issues raised by data storage and sharing).

strong right to information privacy due to stagnation in the rights-based model and a failure to recognize the power of information.

2. *Structural Approach: Something Different*

Consequently, the solution requires a structural approach that reorganizes the distribution of power over personal information between government and corporate entities and individuals.[272] Before proceeding, we must develop the concept of a structural approach.[273] The basis for the term rests on the image of a building foundation. A building's foundation establishes its dimensions at a basic, committed level. It provides the stepping stone for any of numerous potential edifices, but once completed, it also permanently excludes a subset of possible structures. Consider the foundation for a single story residence. The foundation could be laid knowing only the planned dimensions of the home—a point in development where questions about doors and windows are irrelevant. The foundation reveals the limits, and an observer could reasonably conclude that building will not be a skyscraper.

Transposing this analogy on the current analysis, certain features of a structural approach are evident. The approach operates using broad generalizations that facilitate a singular purpose—for example, the analogy's purpose to build a place to live. Furthermore, the approach seeks to create physical barriers that block some purposes—for example, the impossibility of constructing a high-rise on the foundation for a hovel. For information control, the structural principles seek to organize information systems so that physical impediments reduce the feasibility of unfettered government or corporate control over citizens' personal information and ensure data privacy for any resultant system.

Since the structural approach assumes such an abstract perspective and operates from blatant policy choices,[274] the solution would necessarily be legislative rather than judicial.[275] While a rights-based model may be one means to comply with the structural principles, the details of any

272. *But cf.* Bibas, *supra* note 23 (proposing an approach requiring personal information contracts between individuals and data collectors). Given the inequitable power distribution between individuals and data collection groups, *supra* notes 266-68 and accompanying text; *see also* Sovern, *supra* note 16, at 1090-91, 1112 (advocating an opt-in contract with data collectors and noting that it would not significantly reduce the information industry because consumers lack the resources to deal with these matters and marketers have a strong incentive and the resources to convince consumers to opt-in), Bibas's more rights-based approach fails to actually provide individuals substantive protection.

273. *See generally* RAWLS, A THEORY OF JUSTICE (1971) (justifying principles for political systems by the principles' structural consequences that ensure *fairness* for the system's procedures).

274. *E.g.*, *infra* Part V.A.3 (weighing the value of interests in privacy and convenience to formulate a principle of information management).

275. *Cf.* Matthews v. Diaz, 426 U.S. 67, 81 (1976) ("[S]ince a wide variety of classifications must be defined in the light of changing political and economic circumstances, such decisions are frequently of a character more appropriate to either the Legislature or the Executive than to the Judiciary.") (ruling on a standard of review for Congress's social security requirements for resident aliens).

final method of compliance would be irrelevant in considering the underlying principles,[276] similar to the windows and doors in the home analogy. A structural solution should reorient information systems in a way that the solution's underlying principles function as operating facts. In other words, if an information system exists, it complies with the solution's principles because to do otherwise would not be physically, socially, or economically feasible.[277]

For a concrete example at a lower level of abstraction, consider traffic rules, specifically rules regarding traffic lanes. On a two-lane road with traffic traveling in both directions, cars on either side drive in opposite directions. All drivers accept this rule as a pure operating fact because travel in the other lane would not be feasible. This conclusion does not mean that traveling in the other lane would be impossible. The driver could easily pull into the other lane. However, due to the presence of other vehicles, honking admonishments from fellow travelers, or concern for damaging the car, the driver foregoes the option because it would not be physically, socially, or economically feasible.

B. Technology as a Tool

Furthermore, to formulate a structural solution for information control, the solution must respect technology. The second premise recognizes that the risks to privacy from networked databases stem from technological advancement.[278] The risks, however, should not inspire Neo-Luddites or instigate a retreat to technologically-bereft woods.[279] Technology must be acknowledged as a tool, with its products shaped by the purpose for which they were created. A structural solution should use technology to fashion results with an underlying concern for privacy.

Traditional methods of avoidance to maintain anonymity will not suf-

276. *Cf.* RAWLS, *supra* note 273 (arguing that the principles of fairness do not necessitate any specific form of compliance).

277. This Note does not explore the technological feasibility of systems. Accordingly, highly sophisticated technological proposals are not explored. Also, software impediments that increase privacy and security measures that preserve the integrity of data are not considered as aspects of the structural solution. For a starting point on these topics, see Ctr. for Educ. & Research in Info. Assurance & Sec., *Network Security* (last visited Feb. 18, 2000), *at* http://www.cerias.purdue.edu/coast/hotlist/network (linking numerous resources regarding types of security available for information and databases shared over a network); Electronic Privacy Info. Ctr., *EPIC Online Guide to Practical Privacy Tools* (last visited Feb. 18, 2000), *at* http://epic.org/privacy/tools.html (listing software available to protect data shared through diverse network services, such as e-mail and webpages); RSA Security, *RSA Laboratories' Frequently Asked Questions About Today's Cryptography* (last visited Feb. 18, 2000), *at* http://www.rsasecurity.com/rsalabs/faq/index.html (providing educational information on the methods of encryption and authentication available to protect personal privacy).

278. *Supra* Part I.A.

279. Nancy Allen, *Ludditism Today* (last visited Feb. 18, 2000), *at* http://publish.uwo.ca/~nallen1/nlud.htm (describing the Neo-Luddites as opposed to technology that deprives individuals of their humanity and using the Unabomber, Theodore Kaczynski, as an example).

fice in modern society.[280] Only technological solutions can balance interests in convenience and privacy while staying current with the fast-paced innovations for data usage. Yesterday, it was index card files;[281] today, the Internet and networks;[282] tomorrow, perhaps biometric scanners.[283] Therefore, any analysis must explore the possibility that given an impetus and direction to protect privacy, technology could contribute to the overall solution.

IV. Structuring Information Control

Proceeding with a mandate to formulate a structural solution with technological components, the national identification number models from the United Kingdom and South Africa set a useful comparative scale for evaluating principles of information control. The following analysis employs the same organization used when the models were introduced, examining the privacy implications for each country's treatment of information management, privacy enforcement, and citizens' access to information. After formulating a solution and explaining how the resulting principles operate, we can evaluate the potential impact on the United States.

A. Information Management

The United States uses a system of information management characterized by a decentralized network of databases with weak access and privacy restrictions.[284] Due to the weak restrictions, the system approximates a more centralized database.[285] While there is no means available to search the entire network as if it were a single database, easy access allows organizations to collate records with minimal effort, especially since the privacy protections are inadequate to limit the use of social security numbers as identification numbers.[286] This U.S. system developed by balancing the interests in convenience and privacy.[287] An appropriate solution must continue to recognize the need for balance, even though the interests advocate solutions in diametric opposition to each other.

---

280. Swire, *supra* note 13, at 473-74 (describing the harsh chilling effect of financial surveillance on citizens' activities as individuals attempt to minimize exposure to scrutiny by avoiding traceable transactions); *see also supra* notes 54-56.

281. *Supra* note 177 and accompanying text.

282. *Supra* Part I.A.

283. *E.g.*, David E. Kalish, *Eye Scans and Palm Readings Might Become ID of the Future*, OREGONIAN, July 27, 1997, 1997 WL 4193534. *See generally* Woodward, *supra* note 31.

284. *Compare supra* Part II (defining decentralized information management as separate locations or restricted access), *with supra* Part I.A (describing the basic technological underpinnings of the U.S. database network), *and supra* Part I.B.2. (exploring what entities have access to social security numbers in the United States).

285. *Id.*; *supra* notes 35-36 and accompanying text.

286. *Id.*; *supra* Part I.B.2.b.i, ii.

287. *Supra* Part I (explaining the interests in efficiency and privacy that motivate the U.S. debate about social security numbers).

1. Privacy

Due to excessive release of personal information from a centralized database,[288] privacy interests require a solution that uses decentralized information management. A decentralized system provides physical impediments to data access.[289] Each organization must specifically collect the information stored on its database.[290] The collection process may entail direct requests addressed to the individual or indirect requests addressed to other organizations.[291] Either method provides stronger intrinsic privacy protection than a centralized database. Direct requests empower the individual by permitting control over the flow of information to different sources.[292] Indirect requests harbor a potential for protection due to bureaucratic obstacles that block rampant collection of personal information.[293] Whether or not the organization holding the data may be lenient in distributing the information to others, the mere necessity of asking permission imposes an impediment because it requires another person to analyze the legitimacy of information requests.[294] Therefore, interests in privacy press toward a decentralized system.

The United Kingdom uses a database network similar to the United States, but the network differs significantly with regard to access restrictions.[295] Without a national identification number, collating information between the different databases presents a substantial challenge.[296] Furthermore, government and corporate entities must satisfy the Information Commissioner that they have a legitimate purpose for collecting the information and sufficient privacy protections to secure the data from improper use.[297] These additional facets of the United Kingdom's model differentiate it from the U.S. system and impose barriers between databases that make the result truly decentralized.[298]

---

288. *Supra* notes 16-18 and accompanying text (describing concerns raised in the U.S. privacy debates); *see also supra* note 189 (listing the Data Protection Principles enforced in the U.K.)

289. *E.g.*, *supra* notes 181-84 and accompanying text.

290. *E.g.*, *supra* notes 181-84 and accompanying text.

291. *E.g.*, *supra* notes 181-84 and accompanying text.

292. *Supra* Part III.A.1.b (discussing the power of information and noting the struggle of individuals for control over the flow of that information).

293. *E.g.*, *supra* text accompanying note 13 (contrasting the difficulties of collating information by hand with the ease of database queries); *cf. supra* note 18 and accompanying text (listing the elimination of bureaucratic impediments to information collection as a risk of national identification numbers).

294. *E.g.*, *supra* Part II.A.2. Depending on the reviewing agency or firm, the legitimacy analysis would involve diverse factors that may not include privacy interests.

295. *Compare supra* note 284 and accompanying text, *with supra* notes 179-84 (describing a decentralized database system with practical access restricted between separate databases because of incompatible information storage).

296. *Supra* notes 37, 294 and accompanying text.

297. *Supra* notes 189-93 and accompanying text; *see also supra* notes 54-55 and accompanying text.

298. *Compare supra* notes 284-86 and accompanying text, *with supra* notes 181-84 and accompanying text.

In contrast, if characterized as a highly centralized and unrestricted system of information management, South Africa's model would only present a straw-man proposal, felled easily in the interests of privacy.[299] Although that characterization would be premature, a proper categorization of the system is difficult because South Africa has not finalized and implemented the model.[300] Accordingly, in discussing unknown or ill-defined features, this Note extrapolates to fill gaps. In so doing, two aspects in combination indicate strong access restrictions to the centralized database.[301]

The centralized facet of South Africa's model hinges on the collection of all information through smart cards synchronized with a single database.[302] The government's primary purpose for the smart card, however, is to provide a method of verifying identity and personal information.[303] At least according to preliminary understandings, while government and corporate groups may maintain separate databases, the centralized database will only be used for identity verification.[304] It would be inconsistent to allow verification inquiries when the individual to be identified is not present; government and corporate entities would not be able to query the database without the smart card, the key to authenticating identity. Even with the smart card, entities could only verify information.[305] Therefore, citizens retain strong control over the flow of personal information because they possess the key to accessing the database and requests for information would not reveal excess data.

However, South Africa's system should still be considered centralized. The mere existence of the single database used for verification poses a significant risk of "mission creep."[306] For example, enacting one exception to privacy protections for law enforcement to track criminals may lead to another exception for tax agents to trace spending habits. Eventually, the

---

299. *Supra* notes 288-94 and accompanying text.

300. Lesley Stones, *Smart Cards to Replace ID Books in SA in 2001*, BUS. DAY, (S. Afr.) Feb. 1, 2000, 2000 WL 7450599 (indicating that the smart cards should be issued to citizens in the second half of 2001, but noting the history of changes to the proposal since first considered); *see also supra* 191-95 and accompanying text.

301. *Cf. supra* notes 284-86 and accompanying text (stressing, in the context of the U.S. system, the importance of strong access restrictions to a model focused on privacy protection).

302. *Supra* notes 206-12, 215-18, 222 and accompanying text.

303. *Supra* notes 208-12 and accompanying text.

304. *Supra* note 210.

305. *E.g.*, Dep't of Home Affairs, *supra* note 208 (describing the centralized database as a basis for comparison, which implies that government and corporate entities must already possess personal data to compare with the central database). This conclusion may be wishful thinking if technical issues make it impractical to limit queries compared to an alternative that releases a full record for the requesting agency to spend resources parsing. *E.g.*, Oracle, *Database Limits* (last visited Feb. 18, 2000), *at* http://oradoc.photo.net/ora81/DOC/server.815/a67790/ch4.htm (describing the different types of limits on Oracle database use, including limits on the number of queries that can be processed simultaneously). However, the privacy implications of releasing a full record make South Africa's model wholly unappealing. *Supra* note 299 and accompanying text.

306. *Supra* notes 35, 51-52 and accompanying text.

exempted uses outnumber the restricted uses.[307] Therefore, South Africa's model raises inherent difficulties for privacy interests.

2. *Convenience*

In contrast to privacy interests, interests in convenience press for a centralized method of information management because of the greater efficiency.[308] With data stored in a single location or networked in a system of unrestricted access, a centralized database maximizes convenience.[309] Centralized data eliminates bureaucratic restrictions on access to files from other organizations[310] and redundancy in filing, which risks inaccurate or outdated information,[311] but retains the benefit of readily retrievable data.[312]

On this account, the United Kingdom's model fails miserably. The relative anonymity enjoyed by British citizens comes at the price of rampant inefficiency in government services.[313] Redundant collections of information and copious identification cards and numbers prevail.[314] The inefficiency and inconvenience of the system has even triggered a reaction from the U.K.'s government to rectify the situation.[315] An abundance of databases without any simple means of linking the stored information is not conducive to convenience.[316]

On the other hand, South Africa's model preserves the convenience of data storage and sharing. With access to a citizen's smart card, a government or corporate organization can verify the accuracy of information supplied by the individual or other sources.[317] The information would then be stored on separate databases and used confidently to process services

307. *E.g.*, *supra* Part I.B (discussing the steady expansion of uses for the social security number beyond tracking citizens qualified for benefits).

308. *E.g.*, MODERNISING GOVERNMENT, *supra* note 182, ch. 4, 5 (identifying inefficient processes as contributing to dissatisfaction with inconvenient government services and discussing steps to increase system efficiency that would have a corresponding positive impact on convenience).

309. *Supra* note 161.

310. *Supra* notes 289-94 and accompanying text (noting that an organization must contact either the citizen for information or seek another organization's permission for data in a decentralized system).

311. *E.g.*, NASA, *GIS Business Plan* (Feb. 16, 1995), *at* http://gis-www.larc.nasa.gov/bplan/bplan0.html ("Another problem is that of redundant database development & maintenance efforts . . . . Any changes must be entered in three different databases. The information is updated with differing frequency and accuracy.") (conducting a cost-benefit analysis for using Geographic Information Systems technology at Langley Research Center); *cf. supra* notes 40, 44-48 and accompanying text (discussing the dangers of reliance on separated databases generally).

312. *Supra* examples discussed at Part I.A.

313. *Compare* Engel, *supra* note 179 (describing the ability of British citizens under a system without national identification cards to "disappear . . . and be challenged by no one"), *with supra* note 183.

314. *Supra* notes 181, 183.

315. *Supra* note 184.

316. *Compare supra* note 184 and accompanying text, *with supra* note 161.

317. *Supra* notes 206-12, 220 and accompanying text; *see also supra* notes 303-05 and accompanying text.

for the individual.[318] Furthermore, while not part of any current proposal, the citizen could grant an entity limited permission to access requisite data for the purpose of updating files.[319] While this model maintains certain redundancies in the system, it minimizes the risks of inaccurate information and simplifies the process for accessing data.[320] Also, the model safeguards the convenience benefits to the individual by minimizing time expended to request or receive services from government agencies or corporate firms.[321]

3. *Balancing*

Neither system presents a solution satisfactory for both privacy and convenience interests.[322] Yet, one area where the models converge is the emphasis on significant access restrictions,[323] which implicitly includes regulation of both public and private data uses.[324] While each country's implementation differs, both impose procedures to protect their respective database systems from unwarranted access and excessive exposure to personal information, features arguably lacking in the United States.[325] This aspect provides common ground from which to create a balanced system between the United Kingdom and South Africa models.

---

318. This conclusion is an extrapolation from the smart card project as so far developed. *Supra* text accompanying note 300; *see also* analysis used in text accompanying notes 304-05. It would be inefficient for corporate firms to not maintain their own databases, if the government only allowed access to the centralized database for verification purposes. *Supra* text accompanying note 304. However, even with redundant databases, the firms could be assured accurate information by conducting regular verification queries of the centralized database. *Supra* note 311 and accompanying text (raising concerns about redundant databases).

319. Given the need to possess the smart card in order to make inquiries of the centralized database, *supra* text accompanying notes 304-05, and the necessity of regular verification queries to maintain accurate information, *supra* note 317, it would be an inefficient process for the firm to constantly seek out the citizen to make the inquiry. Accordingly, a revocable privilege granted by the citizen for the firm to make regular inquiries possible without requiring the citizen's presence increases convenience.

320. *Supra* notes 214, 243 and accompanying text (describing smart card's easy accessibility to stored data); *supra* note 318 (explaining methods for ensuring accurate data).

321. *Supra* note 319.

322. *Compare supra* notes 296-98 and accompanying text (discussing the United Kingdom's success in furthering privacy interests), *and supra* notes 313-16 and accompanying text (failure to satisfy convenience interests), *with supra* notes 299-302, 306-07 and accompanying text (discussing South Africa's failure to satisfy privacy interests), *and supra* notes 320-21 and accompanying text (success in furthering convenience interests).

323. *Supra* notes 295-98, 300-04.

324. *Supra* notes 185, 197-98, 216-18, 235-39 and accompanying text (indicating that the United Kingdom and South Africa do not significantly distinguish public and private data collection for purposes of privacy regulation). Strong access restrictions to data necessitate regulation of government and corporate entities. Otherwise, the unregulated private information market blossoms so that extensive databases of personal information still exist, risking the same intrinsic dangers as large-scale, networked government databases. *See* Simpson, *supra* note 16. The risks of massive personal information databases inhere without regard to whether the data collector is a public or private entity.

325. *Compare supra* notes 295-98, 301-04, *with supra* Part I.B.2.b.i.

The risk of mission creep critically hinders the adoption of South Africa's centralized database because it lacks a fundamental structural obstacle to protect against significant privacy violations.[326] Therefore, the base model must be a decentralized system. Yet, as the United Kingdom's model demonstrates, decentralized systems suffer from an equally fatal disregard for technology as a tool.[327] The effective bar on data exchange eliminates all benefits from technology, but nets a minimal privacy gain because entities could still gather information manually.[328] Thus, some modification must be made to the United Kingdom's system to realize the technological advantages.

South Africa's proposed model restricts access, in part, by only permitting verification inquiries and update requests utilizing the central database.[329] If so implemented, a database would not communicate any new information when queried by government or corporate entities.[330] This process results in a system that furthers interests in using technology to provide efficient and convenient services.[331] Additionally, those particular aspects of South Africa's model could be easily integrated into the United Kingdom's decentralized database system. If the United Kingdom's procedures for restricting access were relaxed in cases where an organization only sought verification information, then the privacy protections would be maintained without the resulting inconvenience.

While a decentralized database network imposes a physical impediment to potential privacy violations, the verification procedure only balances interests in privacy and convenience.[332] As applied to the United States, this facet of the ultimate solution would require the formulation of significant access restrictions.[333] It would also necessitate eliminating all currently available exceptions and replacing them with a single exception for verification requests.[334]

B. Privacy Enforcement

While the analysis for information management demands a balancing of interests between privacy and convenience, consideration of privacy enforcement procedures and citizens' access to information only require evaluation of the models in the interests of privacy. In the United States, individuals motivate privacy enforcement.[335] While the OMB and the Data

326. *Supra* notes 306-07 and accompanying text.
327. *Supra* notes 313-14 and accompanying text.
328. *E.g.*, *supra* text accompanying note 21 (illustrating that databases facilitate data collection but information would be available for collection manually even without databases).
329. *Supra* notes 317-20 and accompanying text (extrapolating from the current South Africa proposal to justify a model that uses verification only and allows for update permission).
330. *Supra* notes 304-05 and accompanying text.
331. *Supra* notes 317-21 and accompanying text.
332. *Supra* Part IV.A.3.
333. *Supra* notes 323-25 and accompanying text.
334. *Compare supra* Part I.B.2.b.i, *with supra* notes 329-31 and accompanying text.
335. *Cf. supra* Part III.A (discussing the U.S. focus on individual rights).

Integrity Boards mandated by the Privacy Act provide ineffective government oversight,[336] the United States has tended recently to rely on the Federal Trade Commission (FTC) to regulate corporate violations of privacy in grave situations.[337] Since the FTC only concentrates on critical privacy issues, however, the agency does not provide a stable system of enforcement. Thus, ultimate responsibility for privacy falls to a group of people with radically diverse motives.[338] In other words, the United States employs a highly decentralized system of privacy enforcement.

In contrast to the reactive role of the U.S. judiciary in enforcing rights, the U.K.'s Commissioner has an active role in validating the privacy protections employed by public and private organizations.[339] The Commissioner critically analyzes proposed data usage for potential invasions of privacy.[340] Furthermore, the Commissioner responds to any proposed system of information management that could impact citizens' data privacy.[341]

Although not to the extreme of the United States or United Kingdom, South Africa splinters responsibility for privacy between several government agencies. As a result, the agencies rarely give serious consideration to the privacy implications associated with the collection of personal information.[342] Arguably, splitting responsibility for individual privacy into several agencies safeguards privacy interests because multiple organizations may scrutinize uses of personal information for compliance with pri-

336. Schwartz, *supra* note 70, at 597-602 (explaining that the Data Integrity Boards function only to police "housekeeping measures"—nonsubstantive provisions—in the Privacy Act and that the OMB, to the detriment of privacy concerns, focuses on the efficiency of computers to carry out its duties to "supervis[e] federal paperwork, debt collection, and the reduction of the federal deficit").

337. Robert MacMillan, *U.S.-Style Data Privacy Tastes Pretty Good*, NEWSBYTES, Jan. 20, 2000, LEXIS, News Library, NWSBYT File; *see also, e.g.*, Press Release, Fed. Trade Comm'n, FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors (July 10, 2000), *available at* http://www.ftc.gov/opa/2000/07/toysmart.htm; Federal Trade Comm'n, *Statement by Jodie Bernstein, Director, Bureau of Consumer Protection, Federal Trade Commission* (Feb. 16, 2000), *at* http://www.ftc.gov/opa/2000/02/dblclickstajb.htm (acknowledging an investigation into Doubleclick's business practices after privacy complaints leveled at the company).

338. *Compare, e.g.*, Baker v. Dep't of the Navy, 814 F.2d 1381, 1381-82 (9th Cir. 1987) (seeking to purge records through the Privacy Act, believing the files had a detrimental effect on her career), *with* Alcaraz v. Block, 746 F.2d 593, 603 (9th Cir. 1984) (seeking to avoid mandatory disclosure of social security number through the Privacy Act because illegal alien believed that disclosure would ultimately result in deportation), *with* Sutton v. Providence St. Joseph Med. Ctr., 192 F.3d 826, 829 (9th Cir. 1999) (seeking to invoke the Privacy Act to avoid disclosing social security number to employer, believing the number represented the Biblical "Mark of the Beast").

339. *Supra* notes 187-90 and accompanying text.

340. *Supra* notes 189-90, 193 and accompanying text.

341. *E.g.*, *Modernising Government Response*, *supra* note 179 (commenting on the privacy implications of the proposal to change the United Kingdom's information management, *supra* note 184).

342. *Supra* notes 224-25, 230-31 and accompanying text.

vacy protections.[343] However, if governments splinter responsibility for privacy enforcement, then the groups on whom the government places the responsibility must necessarily have other duties and priorities;[344] privacy becomes merely another factor to consider.[345] Further, since other agencies also have a responsibility to protect privacy, any one group may minimize its role in fulfilling that responsibility, reasoning that others will correct any lapses. Inevitably, no agency effectively provides privacy enforcement.

Accordingly, the United Kingdom's system of centralized privacy enforcement provides a better model for structuring a U.S. solution. By vesting authority in a single independent agency whose sole purpose involves privacy protection, the structural solution establishes a massive impediment to invasions of privacy. Government agencies and corporate firms could no longer dominate unsophisticated citizens, who fear the vast market and its exchange and use of personal information,[346] but cannot obtain services elsewhere.[347] The risk of investigation, independently or based on a complaint, increases the cost to government agencies and corporate firms for noncompliance with privacy protections.[348] In the United States, this solution would require the creation of a new government agency responsible only for protecting citizens' privacy, a proposal considered in initial versions of the Privacy Act.[349]

C. Citizens' Access to Information

Turning to the models for citizens' access to information, the United States has developed the most decentralized and restricted system for permitting citizen access. Individuals may only query government databases[350] and must submit a written request directly to each agency that collects personal

343. *E.g.*, *supra* text accompanying note 294 (adding additional levels of scrutiny that may hinder privacy invasions as a side-effect, although not suggesting that responsibility for privacy interests be allocated to those additional levels).

344. *E.g.*, *supra* notes 224-31 and accompanying text (describing the other duties of those South Africa agencies charged to protect privacy).

345. *E.g.*, *supra* notes 223-31 and accompanying text.

346. CONSUMER PRIVACY SURVEY, *supra* note 14, at 71 (noting that 94% of consumers were "very" or "somewhat" concerned about the potential for misuse of personal information); *supra* note 50 and accompanying text; *see also* Encyclopedia Britannica, *Information Processing: Effects on the Economy* (last visited Feb. 18, 2000), *at* http://www.britannica.com/bcom/eb/article/7/0,5716,109287+1+106312,00.html ("Awareness that possession of information is tantamount to a competitive edge is stimulating the gathering of technical and economic intelligence at the corporate and national levels.").

347. *Supra* notes 54-56, 154 and accompanying text.

348. *Compare supra* note 268 (noting that firms have no reason to protect privacy and giving examples where firms have disregarded any concern for individual privacy), *with supra* note 190 and accompanying text (describing the power of the Information Commissioner to pursue investigations and prosecute violations).

349. Schwartz, *supra* note 70, at 596 n.265.

350. Freedom of Information Act of 1966, Pub. L. No. 89-487, 80 Stat. 250 (codified as amended at 5 U.S.C. § 552 (1999)) (government-held information); Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a(d) (1999)) (government-held personal information).

information.[351] However, the need for access to personal information does not end at government services.[352] An inability to access, verify, update, and delete records in private databases may equally infringe citizens' privacy.[353] In most aspects, the United Kingdom resembles the United States.[354]

While South Africa uses a similar system of decentralized access requests,[355] the model's intriguing aspect involves the smart card applications.[356] Although the uses for the smart card are not finalized,[357] it represents the ultimate device for collating personal information stored on government and private databases.[358] The smart card could be programmed to provide an individual with full control over access to information, a significant improvement to the decentralized access methods used in the United States and the United Kingdom.

As a miniature centralized database, however, the smart card risks mission creep.[359] At this point, it will help to invoke the technology premise.[360] Since South Africa's smart card represents a significant advance in identification technology, certain technological aspects of the identification procedure should be explored. The previous discussion rejected only one facet of the smart cards as incompatible with privacy interests—synchronizing the smart card with the centralized database of fingerprints and personal information.[361]

Yet, the smart card maintains a separable, internal identification method that matches the holder's fingerprint with the fingerprint electronically stored on the smart card.[362] If the holder's fingerprint does not

---

351. *Id.*; *see also, e.g.*, 5 C.F.R. § 297.201 (1999) (limiting access to Civil Service personnel records unless written request submitted and identity sufficiently established); *cf.* Dale-Murphy v. Winston, 820 F.2d 1470, 1476-77 (9th Cir. 1985) (requiring request conforming to regulations before even recognizing a claim for access under the Privacy Act).

352. *Supra* Part I.A (describing the problems with large-scale databases as inherent to the systems without regard to the entity that stores the information); *see also* note 346.

353. *E.g.*, Germosen v. Cox, No. 98 Civ. 1294 (BSJ), 1999 U.S. Dist. LEXIS 17400 (S.D.N.Y. Nov. 9, 1999) (dismissing a Privacy Act claim to recover records from American Airlines and New York Telephone related to plaintiff's wire fraud conviction); Steadman v. Rocky Mountain News, No. 95-1102, 1995 U.S. App. LEXIS 34986, at *4 (10th Cir. Dec. 11, 1995) (unpublished table opinion) (dismissing Privacy Act claim in disability discrimination case against plaintiff's former employer).

354. *Compare* Data Protection Act, 1998, ch. 29, § 7 (Eng.), *with* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1897 (codified as amended at 5 U.S.C. § 552a(d) (1999)).

355. *Supra* note 236 and accompanying text.

356. *Supra* Part II.B.3 (discussing the potential for smart cards as means for citizens' access).

357. *Supra* notes 305, 329 and accompanying text (noting that South Africa continues to develop its information control strategy and projecting consistent facets of the strategy from known information, where necessary to fill gaps in the discussion).

358. *Supra* notes 233-43 and accompanying text.

359. *Supra* notes 306-07 and accompanying text.

360. *Supra* Part III.B.

361. *Supra* notes 306-07 and accompanying text.

362. Dep't of Home Affairs, *supra* note 208 (describing one identity verification procedure as "stand-alone verification, which reads the [fingerprint] on the card").

match the stored print, the smart card could be limited to only verification requests.[363] Since the identification measures ensure that only the verified holder of the smart card has complete access, the smart card minimizes the danger of other people appropriating the personal information on the card for purposes beyond those originally conceived for the device.[364] Thus, integrating the technological solutions for identity verification directly into smart cards functions to prevent risks of mission creep.

Privacy concerns necessitate one final modification to the smart card system as proposed in South Africa. Given South Africa's long tradition of identification documents, the country's cultural reaction differs significantly from the responses in the United Kingdom and United States.[365] Accordingly, the structural solution's smart card would not be used for identification purposes. Instead, the smart cards would be supplied to citizens as government-sponsored devices with identity verification safeguards.[366] The smart card's purpose would be specifically to fashion an interface and infrastructure that empowers citizens to access public and private databases containing personal information. The internal fingerprint identification protection, lack of centralized identity verification procedures, and limited purpose for citizens' convenience combine to minimize the possibility of using the smart card as a mandatory identification document.

D. Domestic and International Impact of the Structural Solution for the United States

From this discussion, the following structural principles emerge to guide the establishment of a government system that respects privacy interests in

363. *E.g.*, *supra* notes 304-05 and accompanying text (introducing the verification-only feature).

364. *Compare supra* notes 362-63 and accompanying text (discussing a stand-alone information access and verification device), *with supra* note 306 and accompanying text (relying on the idea that information flows easily between networked systems, *supra* note 51-52 and accompanying text). Although beyond the scope of this Note, the information on the smart card would also require significant procedural protection from police investigation and government appropriation. *See* Simpson, *supra* note 16.

365. *Compare supra* note 205 and accompanying text (describing South Africa's relative comfort with identity documents), *with supra* notes 174-80 and accompanying text (describing the United Kingdom's brief touch with a national identification card and debates over a new card).

366. The smart cards would need to be government-sponsored to facilitate uniform legislation of standard protocols and other infrastructure requirements, similar to the growth of the Internet. Vint Cerf, *A Brief History of the Internet and Related Networks* (last visited Feb. 21, 2000), *at* http://www.isoc.org/internet/history/cerf.html. However, the smart card would also need specific protections from the government. For example, the costs of the system may outweigh the privacy benefits if law enforcement officers could obtain warrants for the information contained on the smart cards. *Cf.* Simpson, *supra* note 16 (describing the FBI's use of an information reference service to circumvent Privacy Act restrictions on government profiling). Since the smart card's role serves to reduce the burden on the citizen for information access, these concerns do not pose a serious difficulty because smart cards are only one means of providing the structural value of centralized information access. Unfortunately, this Note cannot further explore these issues.

the context of technological advances that risk unnecessary and excessive dissemination of personal information.

1. *Information Management*: Governments should structure data distribution so that personal information resides on a decentralized network of databases maintained by individual government agencies or firms. Data sharing of personal information between any databases on the network, public or private, should be restricted to verification requests rather than complete release of records.[367]
2. *Privacy Enforcement*: In addition to allowing individuals to pursue privacy suits in court, governments should structure mechanisms for privacy enforcement by vesting a government agency with the sole responsibility and singular purpose to protect citizens' data privacy.[368]
3. *Citizens' Access to Information*: For the citizen's convenience, governments should issue a smart card or other device capable of centrally organizing an individual's personal information stored on public and private databases. To secure the device from other applications, it should use an internal user identification procedure, access databases directly instead of storing the information on a centralized database, and limit users to verification queries if the user does not pass internal identity authentication.[369]

Taken together, these principles impose significant impediments to invasions of data privacy. If implemented, the principles constitute a set of operating facts that any organization seeking to collect, use, or disseminate information would follow of necessity.[370] Although it would not be impossible to violate the principles, the numerous obstacles would place an overwhelming burden on the organization seeking to maintain the violation, and the diverse checks on the system would pose a high risk of discovery and sanction.

Naturally, these principles do not incapacitate agencies and firms, making invasions of privacy impossible. However, the impediments and checks make privacy violations extremely difficult and discovery probable. An agency or firm may find a means of accumulating vast quantities of data outside the verification-only system; yet the government agency and citizens' smart cards would have the capacity to detect any excessive collection of personal information by a single organization. If the agency or firm also found some method for avoiding oversight—for example, by failing to register their database as a collection of personal information subject to government oversight and smart card data retrieval—then it would be difficult to detect the violations. However, the agency or firm would need to operate in complete stealth on a black market of information exchange because at any public hint of the practices, the government privacy agency could institute an investigation to ensure compliance with privacy principles.[371]

---

367. *Supra* Part IV.A.
368. *Supra* Part IV.B.
369. *Supra* Part IV.C.
370. *E.g.*, *supra* note 277 and accompanying text.
371. *Supra* 348-49 and accompanying text.

Understanding how the impediments function within the structural solution, the potential impact of such a system in the United States unfolds. The most beneficial effect stems from a return to the values inspiring a rights-based model.[372] The structural solution levels the information control inequities by conferring upon citizens an active role in enforcing their interest in personal information. In addition, internationally, the solution would conform the United States to the European Union's data privacy protections.

The structural solution revives the underlying values of the rights-based model in promoting individual autonomy and empowering citizens as active participants in society. In particular, the smart card gives individuals an effective means of policing organizations' use of personal information. This power essentially reorganizes the information control structure so that individuals need not be beholden to agencies and firms for personal information in order to receive services.[373] Agencies and firms may still request information, but even if released to the organization, the individual retains the ability to monitor the use of personal data.

Autonomy necessitates control of identity through personal information.[374] Citizens should have the power to define themselves without unsolicited interference from external sources. Allowing organizations to collect and use personal information strips citizens of the power to define themselves because it places the burden on the citizen to obtain services outside his database profile.[375] The transaction costs to obtain outside information will limit the extent to which a citizen will be able to establish an identity other than the profile controlled by the organization.[376] By using the smart cards and defining their public identity, individuals become an active player in ensuring the consistency and accuracy of both the public and private aspects of an information society.

Moving to the international impact, the United States would comply with protective measures restricting transborder flow of personal information outside the European Union.[377] Since October 1998, the United States had attempted to demonstrate to the European Union that adequate

372. *Supra* notes 257-58 and accompanying text.

373. *Supra* note 156 and accompanying text.

374. *Cf.* Kelley v. Johnson, 425 U.S. 238, 251 (1976) (Marshall, J., dissenting) (arguing that forcing individuals to sacrifice their identity by regulating personal appearance is inconsistent with valuing privacy and autonomy). This use of autonomy should not be confused with the technical usage as the autonomy branch of the right to privacy—"independence in making certain kinds of important decisions." *Supra* note 80 and accompanying text. While the technical use would be limited to decisions related to fundamental activities, *e.g.*, Plante v. Gonzalez, 575 F.2d 1119, 1132 (5th Cir. 1978), the current, broader use refers to any activity reflecting free choice, *supra* note 244.

375. *Cf.* Sovern, *supra* note 16, at 1090-91 (indicating that consumers lack the resources to effectively manage their interaction with businesses).

376. *E.g.*, *id.* at 1074-78 (describing diverse transaction costs that inhibit consumers from opting out of personal information databases kept by firms).

377. Data Privacy Directive, *supra* note 3, art. 25.

protections exist in the United States to safeguard data privacy.[378] The EU did not recognize any sufficiently binding privacy protections in the United States and disagreed with the U.S. policy of self-regulation, which allows businesses to define the methods used to protect privacy.[379] This impasse led to the safe harbor exceptions.[380] In contrast, instituting the principles of the structural solution would likely satisfy the stringent requirements of the Data Privacy Directive.[381] Consequently, by implementing the structural solution, the United States would not be left advocating a position inconsistent with the policies of other developed countries and contradicting its own values in autonomy and an active citizenry.

Conclusion

Advances in technology challenge traditional notions of privacy everyday, provoking a privacy crisis. As personal data becomes the currency of the information age, the importance of recognizing a privacy right in data capable of revealing detailed information about individuals grows. For this reason, national identification numbers serve as an excellent context to explore the technological implications of even small pieces of information and the data privacy models available to safeguard that information.

If it even exists, a right to data privacy in the United States has steadily declined in scope and effectiveness since the 1970s. The United Kingdom enacted strong protections for data privacy, but suffered significantly from an inability to take advantage of the conveniences offered by technological advances. South Africa has embarked on a unique and ambitious project to balance privacy interests while exploiting the improvements of available technology, but the proposal is deeply rooted in a cultural acceptance of identification documents. As yet, none of these countries has implemented a system that reveres individual privacy and benefits from technological advances within a culture that distrusts national identification.

Any effort to structure such a system must organize the flow of information between organizations and individuals so that individuals retain control of the collection, use, and dissemination of personal information. The U.S. right to privacy has been unable to give individuals this form of

---

378. Deborah Hargreaves, *U.S. Aims to Break Data Privacy Deadlock*, FIN. TIMES (London), Jan. 12, 2000, at 8.

379. Sylvia Dennis, *Italy Urges Truce in U.S.-E.U. Data Privacy Battle*, NEWSBYTES, Feb. 9, 2000, LEXIS, News Library, NWSBYT File. *But cf. BBBOnline, FEDMA, Eurochambres Move to Create International Trust Initiative for E-Commerce*, BUS. WIRE, Apr. 23, 2001, LEXIS, News Library, BWIRE File (noting the efforts of European and U.S. business groups to formulate international self-regulation standards for e-commerce).

380. *Supra* notes 3-7 and accompanying text.

381. *Compare* Data Privacy Directive, *supra* note 3 (requiring databases be restricted in duration to limit unwarranted uses and excessive release of information, *id.* art. 6; appointment of controller to ensure compliance with Directive's provisions, *id.* art. 6; and rights conferred on individuals to access stored personal information, *id.* art. 12), *with supra* Part IV (detailing principles for restricting data storage and sharing to limit unwarranted uses and excessive release of information, *id.* at A; appointing a single agency to enforce privacy protections, *id.* at B; and enabling individuals to access stored personal information, *id.* at C).

information control over personal data. Accordingly, a different approach may be required. The privacy right's underlying values, however, should not be ignored.

While both the United Kingdom and South Africa's systems suffer from inadequacies, the countries offer distinct comparative models from which ideas for U.S. modifications could be drawn. An analysis of specific aspects of the countries' approaches to national identification best informs a possible solution. While adopting the United Kingdom's loose database structure and powerful privacy enforcement provisions, the solution's most unique aspect uses a modified version of South Africa's smart card proposal. Bringing these aspects together, the resultant structural principles for a privacy protection framework respect traditional values in individual autonomy and an active citizenry and recent international privacy values. Although theoretical, these principles provide the groundwork for shaping legislative reform to pull the United States out of its privacy crisis and renew commitments to empowering citizens with the ability to control their lives and identity.