Richmond Journal of Law and Technology

Volume 12 | Issue 3 Article 2

2006

Freedom of Information Laws in the Digital Age: The Death Knell of Information Privacy

Ira Bloom

FREEDOM OF INFORMATION LAWS IN THE DIGITAL AGE: THE DEATH KNELL OF INFORMATIONAL PRIVACY

Ira Bloom[*]

Cite as: Ira Bloom, *Freedom of Information Laws in the Digital Age: The Death Knell of Informational Privacy*, 12 RICH. J.L. & TECH. 9 (2006), *at* http://law.richmond.edu/jolt/v12i3/article9.pdf

"With technology, everything just comes faster, smarter, and meaner. But the basics remain the same."[1]

"Issues involving privacy are difficult and inconsistent….In other words, you better think first."[2]

[1] Murder, kidnapping, stalking, and identity theft are all facilitated by the availability to the public of personally identifiable information in the records of state and local governments. A recent Connecticut Supreme Court decision, *Department of Information Technology of Greenwich v. Freedom of Information Commission*,[3] will likely spur freedom of information law requests for public agency databases. Not surprisingly, anxiety and uneasiness about the uncontrolled availability and

---

[*]Professor of Political Science, Lehman College of the City University of New York; B.A. 1964, the City College of the City University of New York; J.D. 1967, Harvard University.
I thank Jennifer A. Kroell, J.D., June 2005, Benjamin N. Cardozo School of Law, for her excellent research assistance.

[1] COL. DAVID H. HACKWORTH & EILHYS ENGLAND, STEEL MY SOLDIERS' HEARTS 401 (2002).

[2] Dakotah Pratt-Hewitt, *Open Government Group Seeks Amendment to Force Payments*, THE LEGIS. GAZETTE, Oct. 20, 2003, at 2 (quoting Robert Freeman, Executive Director, New York State Committee on Open Government).

[3] Dep't of Info. Tech. of Greenwich v. Freedom of Info. Comm'n, 874 A.2d 785 (Conn. 2005) (affirming order to release Town of Greenwich GIS database in electronic format in response to request under Connecticut Freedom of Information Act). *See infra* notes 80-93 and accompanying text.

dissemination of personal information, particularly the collection and use of personally identifiable information,[4] have proliferated with the advance of the internet and the creation of large databases by corporations.[5] These anxieties have been energized by recent revelations about the easy availability of personal information and of serious breaches of data security.[6] Congress and the states have enacted a limited patchwork of

[4] Commenting about the reluctance of political campaigns to use online advertising, a political scientist wrote:

> Campaigns would dive into online advertising at the risk of antagonizing public opinion on the rising policy issue of individual privacy. . .Online privacy activists . . .warned ordinary users to be suspicious of how ads happened to appear before them and to be careful about volunteering information about themselves.

MICHAEL CORNFIELD, POLITICS MOVES ONLINE: CAMPAIGNING AND THE INTERNET 44-45 (2004).

[5] *See, e.g.*, Carol Marie Cropper, *Between You, the Doctor, and the PC*, BUS. WK., Jan. 31, 2005, at 90 (describing shift from paper to computerized health records with push to develop network and internet access to records and concomitant privacy concerns); Diana Jean Schemo, *A Federal Proposal to Keep Data on All College Students Raises Questions of Privacy*, N.Y. TIMES, Nov. 29, 2004, at A19 (discussing the Federal Government proposal to create new database of enrollment records, including social security numbers, of all college and university students in U.S. raised privacy concerns among a number of groups); Matthew L. Wald, *Airline Gave Government Information on Passengers*, N.Y. TIMES, Jan. 18, 2004, at 16 (revealing that, without notice, Northwest Airlines gave data to NASA about ten million 2001 passengers for post 9/11 research seeking to determine "if the government could mine the data to identify terrorists"); *see also* ROBERT O'HARROW, JR., NO PLACE TO HIDE (2005) (examining competing interests of security and privacy and the relationship between government and private companies with extensive databases and data-mining capabilities that often serve as government contractors, giving government access to information without the restrictions often placed on government actions); *infra* note 50 and accompanying text. Professor Cornfield noted the Internet's contribution to focusing increasing attention to privacy concerns: "[I]t is premature to consider whether any issues have gained or lost public force from the Internet, with the important exception of privacy protection." CORNFIELD, *supra* note 4, at 100.

[6] *See, e.g.*, Tom Zeller Jr., *Personal Data For the Taking: Students Surfing Public Records Learn It's Easy to Find Out a Lot*, N.Y. TIMES, May 18, 2005, at C1 (reporting that students in a computer security course at Johns Hopkins University, using only legal, public sources of information (including, among other records, land deeds, occupational licenses, voter registrations, and court records), were able to obtain "multiple layers of information" about Baltimore citizens); Eric Dash and Tom Zeller Jr., *Mastercard Says 40 Million Files Are Put At Risk*, N.Y. TIMES, June 18, 2005, at A1; Eric Dash, *Lost Credit Data Improperly Kept, Company Admits*, N.Y. TIMES, June 20, 2005, at A1 (reporting about security breach resulting in exposure of 40 million credit card accounts and 200,000 stolen records at payment processing company used by Mastercard and Visa

laws and regulations seeking to control the availability and use of personally identifiable information by the Federal Government and by corporate enterprises; a few of the federal laws, however, preempt more aggressive state laws.[7] Even more limited, however, have been the very few efforts to control the dissemination of information by state and local

to facility card transactions). A major business publication reported in mid-2005 that 46.5 million Americans were subject to privacy breaches during the first half of 2005. *See The Big Picture*, BUS. WK., July 4, 2005, at 9; *see also*, Kevin Poulsen, *Gone Missing*, WIRED, July 2005, at 032 (reporting upon "dataspills" during the first five months of 2005, with 5,520,000 records lost, 2,029,600 attributed to hackers, but 3,490,400 attributed to missing or stolen media or fraud). The data breach problems continued into 2006, with People's Bank of Connecticut reporting the loss of a tape with 90,000 customer social security numbers and other confidential data, following shortly after the loss by LaSalle Bank Corp. of a tape containing information about two million residential mortgage customers. John Christoffersen (AP), *People's loses data on 90K customers*, GREENWICH TIME, Jan. 12, 2006, at B1.

[7] One example of preemption is the Fair Credit Reporting Act, which permanently prevents states from enacting laws regarding the privacy of personal financial information that are tougher than the Federal laws. Pub. L. No. 108-159, 117 Stat. 1952 (codified in 15 U.S.C. § 1681). In a challenge by the American Bankers Association of the affiliate information sharing provisions of the California Information Privacy Act, the Ninth Circuit Court of Appeals ruled that the Fair Credit Reporting Act's affiliate-sharing preemption clause preempted the California Act insofar as it attempted to regulate communication of "information" between affiliates. American Bankers Association v. Gould, 412 F.3d 1081 (9th Cir. 2005). For a discussion of the politics surrounding its passage, see *Financial Privacy*, CQ WKLY., Dec. 13, 2003, at 3110. *See also* Mary J. Hildebrand & Jacqueline Klosek, *Recent Security Breaches Highlight the Important Role of Data Security in Privacy Compliance Programs*, 17 INTELL. PROP. & TECH. L. J., 20 (2005) (reviewing Federal privacy and data security requirements); Paige Norian, Comment, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond*, 52 CATH. U. L. REV. 803, 803-06 (2003) (noting that Congress has left several gaps in existing online privacy protection that could be remedied by a comprehensive Federal law, such as the Online Personal Privacy Act or the Consumer Privacy Protection Act); Neal R. Pandozzi, *Beware of Banks Bearing Gifts: Gramm-Leach-Bliley and the Constitutionality of Federal Financial Privacy Legislation*, 55 U. MIAMI L. REV. 163, 170 (2001) (arguing that although Title V of the Gramm-Leach-Bliley Act appears to increase financial privacy, it does not actually do so, due to many loopholes and exceptions). The financial services industry is seeking to convince Congress to enact a law preempting 23 state data breach security laws. Jacob Freedman, *Industry Seeks One Law On Data Breach Alerts*, CQ WKLY., Feb. 6, 2006, at 314. On March 16, 2006, the House Financial Services Committee approved H.R. 3997, which would set a national standard–"reasonably likely" chance that the information could be misused–for notifications about data security breaches and preempt state laws. Michael R. Crittenden, *Bill Sets Standard for Data Security*, CQ WKLY., Mar. 20, 2006, at 775. *See infra* note 112.

governments within the United States.[8] In the contest between privacy and availability of data, availability is prevailing in the United States. The lack of a unified data privacy policy within the United States is in sharp contrast to the comprehensive European Union (E.U.) Privacy Directive, which applies to both public and private entities within the E.U. countries.[9]

[2] Although much is being written about threats to informational privacy, the literature lacks a careful analysis of the countervailing legal mandates and culture created by state Freedom of Information Laws and Acts (FOILs or FOIAs) for disclosure of information, including personally identifiable information, held by state and local governments in many databases.[10] Magnified by the impact of advances in the use of digital technology, dissemination of these databases through FOILs offers a wealth of often readily available information about residents over which the affected residents have virtually no control.

[3] FOILs are in effect for all fifty states and the Federal Government.[11] Enacted primarily during the 1960's, at a time when state and local governments maintained only a few comprehensive electronic databases that could be accessed only by punch cards and that produced cumbersome paper printouts, FOILs included few provisions addressing their potential impact upon the privacy of personal information about residents.[12] Over the years, FOILs have been amended to take into

[8] *See infra* Section IV.B.1 and accompanying text.
[9] Council Directive 95/46, 1995 O.J. (L 281) (EC). The lack of a unitary U.S. policy reflects the difficulty the U.S. political structure creates for enacting comprehensive, national social legislation. *See, e.g.*, CHARLES NOBLE, WELFARE AS WE KNEW IT: A POLITICAL HISTORY OF THE AMERICAN WELFARE STATE 3 (1997) (analyzing the impact of the political structure of government in the United States upon attempts to create or continue national social service programs).
[10] A striking example is to be found in a chapter of a book addressing issues of privacy and security following 9/11, which, in discussing data users who can force access to data in government databases, mentions discovery and court-issued subpoenas but fails to mention FOILs. George T. Duncan, *Exploring the Tension Between Privacy and the Social Benefits of Governmental Databases, in* A LITTLE KNOWLEDGE: PRIVACY, SECURITY, AND PUBLIC INFORMATION AFTER SEPTEMBER 11 74 (Peter M. Shane, John Podesta, & Richard C. Leone eds., 2004).
[11] *See* Roger A. Nowadzky, *A Comparative Analysis of Public Records Statutes*, 28 URB. LAW. 65 (1996) (summarizing key provisions of the state FOILs).
[12] *See infra* Section III.

account information and data held by government agencies in electronic form.[13]

[4] Databases, however, have changed significantly since the enactment of the original FOILs. Now state and local governments increasingly create comprehensive databases, for purposes of efficiency and improved "customer" service, containing in electronic, digital form vast amounts of personal data about residents within their jurisdiction. These databases are available for viewing and copying in digital format in accordance with the FOILs. The privacy implications for residents have been given little consideration or short shrift when they have been considered.

I. INTRODUCTION

[5] Paradoxically, the combination of electronic databases now held by state and local governments in digital form, the personal computer, computer networks, the internet, and FOILs may present the greatest threat to information privacy and to privacy more generally, a threat significantly greater than that created by corporate or governmental use and misuse of personally identifiable information. In reality, publicly held data obtained under FOILs provide the sources for much of the corporate databases,[14] which, in turn, are sometimes repackaged and sold to governmental agencies.[15] This article will address the privacy implications of these

[13] *See infra* note 30 and accompanying text.

[14] *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1149 (2002).

[15] *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Data for Law Enforcement*, 29 N.C. J. INTL'L. & COM. REG. 595, 596-97 (2004) (describing the sale by commercial data brokers of personal information–often drawn from public records–to law enforcement agencies); *see also infra* note 50 and accompanying text. ChoicePoint is described as "perhaps the world's largest private intelligence operation….ChoicePoint identifies the patterns and links and potential tendencies much faster, and with a sweep that would make James Bond's colleagues envious." O'HARROW, *supra* note 5, at 156. More recent events suggest that Federal agencies may directly be holding and using commercial data. Eric Lipton, *More Privacy Questions for Air Safety Agency*, N.Y. TIMES, June 16, 2005, at A25 (reporting upon inquiry by the Department of Homeland Security Privacy Office regarding whether the Transportation Security Administration used data from private companies inappropriately, including whether private commercial data with detailed information about passengers was stored in the government computer system). ChoicePoint, however, suffered a security breach in early 2005, affecting records involving 140,000 people in all fifty states. Hildebrand & Klosek, *supra* note 7, at 20.

developments at the state and local government level by analyzing what public officials and administrators are doing and the consequences created by the FOILs, with particular emphasis upon the states of New York and Connecticut as examples of two partially contrasting views, while also suggesting potential solutions.

[6] Part II will appraise the accelerating use of large digital electronic databases by public administrators at the state and local level, which is the source of the threat to information privacy. Although considerable attention has been paid to these issues at the Federal Government level, and Congress has enacted the Privacy Act[16] to address some concerns about Federal Government databases,[17] there are fifty state governments and over 87,500 local governments of various types in the United States.[18] Understandably, it is easier to focus on one – the Federal – government's actions, but it is these 87,500 governments that are involved in most of the aspects of day-to-day governing that produce an enormous volume of records, including much personally identifiable information.[19] Examples of such electronic data systems in use in many localities will be examined.

One year later ChoicePoint reached a $15 million settlement with the Federal Trade Commission, which included $10 million in fines and $5 million for consumer compensation for consumers who suffered "real damages" as a result of the ChoicePoint breach. Tom Zeller Jr., *U.S. Settles With Company On Leak of Consumers' Data*, N.Y. TIMES, Jan. 27, 2006, at C3.

[16] Privacy Act of 1974, 5 U.S.C § 552a (2000).

[17] *See* Damien Cave, *Age 16 to 25? The Pentagon Has Your Number, and More*, N.Y. TIMES, June 24, 2005, at A18 (reporting that since 2002 the Defense Department and a private contractor have been building an extensive database of 30 million 16 to 25 year olds for military recruitment purposes, possibly in violation of the Privacy Act because no public notice was made until May 2005). *But see* Freedom of Information Act, 5 U.S.C. § 552(b) (2000); USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of U.S.C.). The Privacy Act does not apply to the Freedom of Information Act, and it was amended by the USA PATRIOT Act. Furthermore, whether the Privacy Act is consistently adhered to is another concern.

[18] U.S. DEPT. OF COMMERCE, CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES 258-59 (2001), *available at* http://www.census.gov/prod/2002pubs/01statab/stlocgov.pdf (including 3,043 county governments, 19,372 municipal governments, and 16,629 township and town governments). In some areas, residents come under the jurisdiction of several local governments, each setting its own policies and practices.

[19] This article will not address the additional issues created by the practice of many state and local governments to embark upon public-private partnerships or to "contract out" or delegate aspects of their functions and responsibilities to private entities (for profit or not for profit), thus leaving private contractors with databases of personally identifiable

information about their residents. *See, e.g.*, Gillian E. Metzger, *Privatization As Delegation*, 103 COLUM. L. REV. 1367 (2003) (questioning "whether delegations of authority to private entities are adequately structured to enforce constitutional constraints on government power").

There is increasing emphasis in public administration on the need to develop collaborative relationships with the private and non-profit sectors through networking in order to deliver services more efficiently and effectively. *See* STEPHEN GOLDSMITH & WILLIAM D. EGGERS, GOVERNING BY NETWORK: THE NEW SHAPE OF THE PUBLIC SECTOR (2004). Although the authors recognize that data privacy concerns are a potential barrier to integrated public-private service delivery, they address the concerns in only two pages (of 188) of text and present responses to the concerns that border on the naive. *Id.* at 103-106.

Several states – including Connecticut, Florida, Ohio, and Pennsylvania – supported initially by Federal funding, have been developing Matrix [Multistate Anti-Terrorism Information Exchange], a controversial database that relies upon both public and private databases to provide police with immediate access to public records and commercially collected information about people in the United States. David Royse, *Police Still Using Matrix-type Database*, CENTREDAILY.COM, July 11, 2005, http://www.centredaily.com/mld/centredaily/news/nation/12105910.htm.

Governments, particularly the Federal Government, are also outsourcing the collection of information and records. "By outsourcing the collection of records [to corporations such as ChoicePoint and Lexis-Nexis], the government doesn't have to ensure the data is accurate, or have any provisions to correct it in the same way it would under the Privacy Act." O'HARROW, *supra* note 5, at 137. A high-ranking official – the Assistant Director heading the New York office – of the Federal Bureau of Investigation also expressed concerns about the private corporations: "There are all kinds of oversight and restrictions to the federal government, to Big Brother, going out there and collecting this type of information. Yet there are no restrictions in the private sector to individuals collecting information across this country, which potentially could be a problem for the citizens of this country." *Id.* at 280. One prominent practicing attorney, however, was not as sanguine about government's use of information obtained from the private sector, criticizing the "lack of principles to guide government use of private sector data. This will be big with the renewal of the PATRIOT Act." Barbara Yuill, *Experts Say Identity Theft Ranks High Among Privacy, Security Topics for 2005,* U.S. LAW WK., Jan. 25, 2005, at 2431.

The private entities, in turn, are increasingly outsourcing parts of their operations to other countries, raising further concerns about data security. *See, e.g.*, Pete Engardio et al., *Fortress India?*, BUS. WK., Aug. 16, 2004, at 42. The protection of consumer data outsourced to other countries is becoming a leading issue, growing in prominence and attention. Yuill, *supra* note 19, at 2430, 2431; *see also* Jacqueline Klosek, *Data Privacy and Security Are a Significant Part of the Outsourcing Equation*, 17 INTELL. PROP. & TECH. L.J. 15, 15 (2005) (reviewing U.S. privacy law requirements implicated by

[7] Although these databases include significant personally identifiable information, very limited attention is being given by public administrators to the privacy and security implications of their use.[20] Few local governments, for example, have a designated, full-time chief privacy officer.[21]

[8] What are the privacy consequences of the convergence of the digital age in public administration and FOILs? Prior to the electronic age, considerable effort often had to be exerted to access the information available under FOILs, which was accessible only in paper format, in or

offshore outsourcing arrangements); Richard Raysman & Peter Brown, *Privacy and Data Security in Local and International Outsourcing*, N.Y. L.J., Feb. 14, 2006, at 3 (emphasizing importance of corporations engaging in due diligence when negotiating outsourcing agreements involving personal information).

[20] A review of a series of books regarding management of information technology – including both theoretical and "hands-on" approaches – designed to provide guidance for public managers and for students of public administration provides telling examples. A CQ Press book of 174 pages includes only one paragraph and one additional sentence, a total of four sentences, devoted to privacy issues. KATHERINE BARRETT & RICHARD GREENE, POWERING UP: HOW PUBLIC MANAGERS CAN TAKE CONTROL OF INFORMATION TECHNOLOGY 125, 173 (2001). A Brookings Institution book that explores how public managers use information technology in complex organizations mentions privacy only in its last two pages. JANE B. FOUNTAIN, BUILDING THE VIRTUAL STATE: INFORMATION TECHNOLOGY AND INSTITUTIONAL CHANGE 205-06 (2001). A more applied book of 214 pages, published by the International City/County Management Association (ICMA), makes no mention of privacy issues. JERSOME A S CHULZ, INFORMATION TECHNOLOGY IN LOCAL GOVERNMENT: A PRACTICAL GUIDE FOR MANAGERS (2001); *see also* GOLDSMITH & EGGERS, *supra* note 19. A limited but more thoughtful discussion of privacy issues is presented in JOHN O'LOONEY, LOCAL GOVERNMENT ON-LINE: PUTTING THE INTERNET TO WORK 92–96 (2000). In contrast, a leader of the e-business movement has recognized the significance of privacy issues:

> [O]ne of the great conundrums of e-business is that it gives enterprises a powerful new capability to capture and analyze massive amounts of information . . . so they can serve individual customers more effectively. Yet this very capability troubles some people, who see it as a means to disclose or exploit their personal information. These are legitimate and very real concerns, and they must be addressed if the world of e-business is to reach its full potential.

LOUIS V. GERSTNER, JR., WHO SAYS ELEPHANTS CAN'T DANCE? INSIDE IBM'S HISTORIC TURNAROUND 328 (2002).

[21] *But see* GERSTNER, *supra* note 20, at 328–29 (including a memorandum from IBM Chairman and CEO reporting creation of position of Chief Privacy Officer and noting that privacy is, at its core, a policy issue not a technology issue).

through agency offices, and agencies were authorized by law to charge per page fees for copies.[22] The information available under FOILs thus was subject to "practical obscurity," the consequences of which were quite significant:

> When records data are accessible only by physical means (that is, by visiting government offices), the costs of travel and the time required to go through paper documents one by one will limit information gathering. Also, it is difficult to remain anonymous while gathering information systematically under the eye of government staff.[23]

The concept of practical obscurity is recognized by the United States Supreme Court. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Court upheld the Department of Justice's and F.B.I.'s decision to deny the request of journalists for an F.B.I. rap sheet compiling conviction records from several states on the grounds that its release would constitute an unwarranted invasion of privacy, although the individual entries included within the rap sheet had been publicly available. [24] The Court succinctly explained the key concern as "whether the *compilation* of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information."[25] Now, the privacy protective consequences of practical obscurity have been obliterated because the extensive use and availability of information in electronic, digital databases create much more data, which then become more readily available to the public. The threat to privacy is increased by the ease of data merging, data matching and data profiling.

---

[22] *See, e.g.*, CONN. GEN. STAT. § 1-212(a)(1) (2004) (providing an example of a fee not to exceed twenty-five cents per page); N.Y. PUB. OFF. LAW § 87(1)(b)(iii) (2005) (providing an example of a fee not to exceed twenty-five cents per photocopy).

[23] O'LOONEY, *supra* note 20, at 92. Paradoxically, more than three decades ago the use of computerized databases to store information made access more difficult because it often eliminated paper files and access to these databases was quite cumbersome. U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 21 n.7 (1973).

[24] United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762–64 (1989).

[25] *Id.* at 764 (emphasis added).

[9] Strikingly, residents have little or no control over the handling and disposition of the information and usually no knowledge of the distribution of digital information about them.[26] The implications for privacy of residents are enormous, as is the potential use of data for criminal activities such as kidnapping,[27] murder, identity theft, and stalking.[28]

[26] Concern about the rights of those included in databases was expressed more than thirty years ago in a major Federal Government report, but in the interim state and local governments have lost sight of these issues:

> An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it.

U.S. DEP'T OF HEALTH, EDUC. & WELFARE, *supra* note 23, at 40–41.

[27] A rare expression of editorial concern about personally identifiable information available on the internet appeared following the kidnapping of a very wealthy financial executive in Greenwich, Connecticut. Editorial, *Kidnapping Indicates New Realities*, GREENWICH TIME, Jan. 19, 2003, at A16. The same newspaper, however, appears to misunderstand completely the significance and consequences of the Geographic Information System [GIS] litigation with which the town is involved. Editorial, *Is Appeal Justified in Map-Access Case?*, GREENWICH TIME, Jan. 18, 2004, at A16 (questioning the town's decision to appeal adverse Superior Court decision). *See infra* notes 68–93 and accompanying text. In a series of articles published in the newspaper during "Sunshine Week," March 12-18, 2006, the writers emphasize the availability of government records and disparage concerns about privacy. *See, e.g.*,Vesna Jaksic, *Government Information; There just for the asking*, GREENWICH TIME, Mar. 14, 2006, at A1.

The victim of the kidnapping–Edward Lambert–was later the subject of the cover story in a national business magazine, a story which begins by describing the tight security now surrounding Mr. Lambert. Robert Berner, *The Next Warren Buffett?*, BUS. WK., Nov. 22, 2004, at 144. Needless to say, most people do not have the resources to provide themselves with this level of private security. Consequently, wide dissemination of information about their homes and properties poses a much greater threat to them.

[28] *See, e.g.*, Harry A. Valetk, *Reclaiming Privacy*, N.Y.L.J., May 13, 2003, at 5 (citing examples of publicly available data leading to instances of stalking and identity theft); *see also* Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1006-08 (N.H. 2003) (noting consequences of stalking and identity theft, and determining on certified question that, following a workplace murder made possible by data searches, an investigative service which supplied the key information to the killer may be liable).

[10] Part III will analyze the use of state FOILs by members of the public to access the information within these state and local government databases, the key issue to address in protecting information privacy. The operation of the FOILs in New York and Connecticut will be considered as examples. These neighboring states have taken somewhat different approaches to the implementation of their FOILs. New York is recognizing in a modest way some of the privacy concerns of its residents, but Connecticut continues to implement its open records policies with seemingly little or no concern for the privacy of its residents.

[11] FOILs make information held by government agencies available to the public, with very limited exceptions. Their emphasis upon open government creates a presumption that government-held information is available for public review and copying.[29] FOIL amendments in many states now require that data held by agencies in electronic format be made available in electronic format at minimal cost.[30] Most FOILs give little, if any, consideration to their impact upon the privacy interests of residents from and about whom data has been collected.[31]

[12] As the digital age and the internet developed, however, FOILs have become subject to a phenomenon that Professor Lawrence Lessig, in the context of copyright, has labeled technological inversion.[32] "Technological inversion happens when a set of values originally

[29] *See, e.g.*, Superintendent of Police v. Freedom of Info. Comm'n, 609 A.2d 998, 1000 (Conn. 1992) (holding that in keeping with the policy of FOIA favoring disclosure and requiring that exceptions to disclosure be narrowly construed, city police department did not satisfy burden of proving municipal permits to carry pistols were similar to exempt medical and personnel files); Capital Newspapers v. Whalen, 505 N.E.2d 932, 935-37 (N.Y. 1987) (holding that personal and unofficial documents intermingled with official government files in office of Mayor of City of Albany are records subject to disclosure under FOIL).

[30] *See, e.g.*, CONN. GEN. STAT. § 1-211(a) (2004); Brownstone Publishers, Inc. v. New York City, 550 N.Y.S.2d 564, 566 (1990) (holding that in response to FOIL request by publishing company, New York City department ordered to provide records on computer tape rather than hard copy).

[31] Few states have privacy laws similar to the U.S. Privacy Act, which, in any event, do not supersede the FOILs. *See* 37A AM. JUR. 2d *Freedom of Information Acts* § 410-413 (dealing with state privacy acts). Some states have enacted general statutes that establish fair information practices dealing with the government's processing of personal information. PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 131 (1996); *see, e.g.*, CAL. CIV. CODE § 1798 (2004); *infra* note 112 and accompanying text.

[32] Lawrence Lessig, *The Creative Commons*, 55 FLA. L. REV. 763, 766-767 (2003).

protected . . . get flipped because the technology embedding those values changes. The world becomes the opposite of what it was, not because politicians have changed the law or the Constitution, but because technologies have changed the interpreted context."[33] Digital technology has made the ability to obtain, collect, compile, manipulate, mine, and transfer data vastly easier than it was thirty-five to forty years ago when most FOIL laws were enacted and consequently has made possible data mining and analysis that were, in a practical sense, not feasible thirty-five years ago.[34]

[13] Is the release of these publicly held databases containing personally identifiable information consistent with the original purposes of FOILs? The purposes of the FOILs will be appraised. FOIL administrators and advocates almost unthinkingly reject any perceived threats to openness (transparency) and seek to apply FOILs blindly to electronic databases of personal information, a telling example of technological inversion. FOIL administrators and review bodies rely heavily upon the presumption of openness and are loath to reject requests for information upon other than the clearest statutory mandates.[35] Court decisions have generally deferred

[33] *Id.*

[34] The power of digital technology is demonstrated by the Federal Bureau of Investigation's initiative to digitize millions of fingerprint cards and connect law-enforcement agencies to the huge new database of fingerprints. The new system "can scan its 46 million sets of prints in minutes, a process that used to take six months by hand." Lorraine Woellert, *Streamlining: FBI*, BUS. WK., Nov. 24, 2003, at 96; *see also* O'HARROW, *supra* note 5, at 43 (quoting Paul Saffo of the Institute for the Future, commenting upon the advance in computing power, paired with the internet: "It used to take an army of gumshoes to do what an individual can do clicking their keyboards in a matters of minutes"). In contrast, in 1973 a Federal Government report stated:

> The possibility of using a large computer to assemble a number of data banks into a "master file" so that a dossier on nearly everybody could then be extracted is currently remote, since the ability to merge unrelated files efficiently depends heavily upon their having many features of technical structure in common, and also on having adequate information to match individual records with certainty….At the present time, however, compiling dossiers from a number of unrelated systems presents problems that few organizations, and probably no organizations outside of government, have the resources to solve.

U.S. DEP'T OF HEALTH, EDUC. & WELFARE, *supra* note 23, at 20-21.

[35] *See, e.g.*, Dir., Ret. & Benefits Servs. Div. v. Freedom of Info. Comm'n, 775 A.2d 981, 987 (Conn. 2001) (noting "that there is an overarching policy underlying the [act]

to these agency actions.[36] This part will also examine a mirror-image problem, the sale of personal information databases by state and local governments.

[14] Part IV will then consider what solutions are available to control the release and dissemination of personally identifiable information notwithstanding the FOILs. States and municipalities may be able to prevent dissemination, although not release, of information within many electronic databases through the judicious use of copyright law.[37] Residents who do not wish personally identifiable information released to the public may seek to avail themselves of United States statutory and Constitutional protections. A handful of Supreme Court cases have addressed the question of the use by and release of personally identifiable information collected in electronic databases by state and local public agencies.[38] Unlike transactional information voluntarily given to corporations during commercial transactions, residents are forced to disgorge personal information to state and local governments under legal compulsion,[39] to exercise their constitutional rights and civic responsibilities to vote and serve on juries, to obtain essential documents and authorizations,[40] to receive public services, and to use government facilities and services.[41] Should they subsequently forfeit all control of the disposition of the information so provided? There are potential Constitutional remedies available. Part V will offer concluding thoughts.

II. ELECTRONIC DATABASES AND PUBLIC ADMINISTRATION: THE THREAT TO DATA PRIVACY

favoring disclosure of public records. It is well established that the general rule under the [act] is disclosure, and any exception to that rule will be narrowly construed.") (internal citations omitted).

[36] *See, e.g.*, Davis v. Freedom of Info. Comm'n, 790 A.2d 1188, 1191 (Conn. 2001) (noting that "[o]rdinarily, great deference is given to the construction given a statute by the agency charged with its enforcement" and that "[a]n agency's factual and discretionary determinations are to be accorded considerable weight by the courts"); *see also* 37A AM. JUR. 2D *Freedom of Information Acts* § 569 (2004) (citing cases in which deference is paid to agency review).

[37] *See infra* section IV.C.

[38] *See infra* section IV.B.2.

[39] Examples include school registration, vaccination records, and drug use.

[40] Documents include driver's licenses, vehicle registrations, marriage licenses, real property title, welfare benefits, etc.

[41] Examples include parks and recreational facilities, senior citizen centers, and libraries.

A. STATE AND LOCAL GOVERNMENT DATABASES

[15] Governments have maintained records about people within their jurisdiction since time immemorial. For the most part, such records were limited and kept confidential. As government record keeping grew and became more commonplace during the mid- to late-nineteenth century, public resistance to the disclosure of the information also grew, and courts and legislatures supported limitations on public access to the information.[42]

[16] The world of information collection, however, changed dramatically after World War II with the invention of the mainframe computer, which enabled the systematic storage of large amounts of data in databases.[43] A second revolution began in the 1980's and continued into the 1990's with the advent of digital technology, personal computers, and the internet. As a consequence, information, including personally identifiable information, is now maintained and made available in electronic format in response to FOIL requests and for other purposes. In such form the data can be easily transferred and recombined with other available data.[44] It also can be transported or stored easily in media such as CDs and floppy disks. It can be conveyed thereafter through telephone, cable, and fiber optic networks, as well as through wireless networks (wi-fi). In addition, information previously available only in paper records in an office during regular business hours can now be posted to the internet for all to see, copy, and transfer. Professor Randall Davis[45] has observed:

> This trio of technological developments–digital information, computer networks, and the Web–are together the source of profound changes in society. Digital

---

[42] Note, *The Right to Privacy in Nineteenth Century America*, 94 HARV. L. REV. 1892, 1907 (1981).
[43] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1402 (2001). The first commercial sale of a computer was to the U.S. Census Bureau in 1951. SCHULTZ, *supra* note 20, at 5.
[44] *See, e.g.*, Adam Liptak, *A Web Site Causes Unease in Police*, N.Y. TIMES, July 12, 2003, at A12 (describing how a police critic posted, on the internet, Washington State police officers' addresses, home phone numbers, and social security numbers obtained from records of voter registrations, property, motor vehicle, and other official records).
[45] Professor of Computer Science at M.I.T.

> information radically changes the economics and character of reproduction; computer networks radically change the economics and character of distribution; and the Web radically changes the economics and character of publication.[46]

Digital technology converts words and numbers (as well as sounds and images) into data bits and bytes, and the converted data instantaneously can be transmitted electronically, monitored, copied, merged, and duplicated. "Information in digital form is orders-of-magnitude easier, faster, and cheaper to reproduce than is information in analog form (for example, hard copy)."[47] Information available in a digital format is subject to many fewer limitations. "Digital copies are…perfect, so each one in turn can be the *seed* for additional perfect copies, quite unlike the situation with traditional media like photocopies."[48]

[17] From a less theoretical perspective, Louis Gerstner, former Chairman and CEO of IBM, has commented:

> It's already clear that a networked world raises many issues, such as the confidentiality of medical or financial records, or the freedom of expression v. protections of personal privacy. Think about the privacy implications of what's coming. What happens to personal privacy in a world of Internet-enabled cars that monitor our movements at all times; cell phones that continuously report their location; or Net-connected pacemakers and other medical devices that are gathering real-time data on our heartbeat or blood pressure, cholesterol level or blood-alcohol content? Who's going to have access to that most personal profile of you–your physician alone? Law enforcement agencies? An insurance provider? Your employer or a potential employer?[49]

---

[46] Randall Davis, *The Digital Dilemma*, 44 COMMUNICATIONS OF THE ACM 77, 79 (2001).
[47] *Id.* at 78.
[48] *Id.* (emphasis added).
[49] GERSTNER, *supra* note 20, at 350 (discussing the future of e-business); s*ee, e.g.*, Amy Harmon, *Lost? Hiding? Your Cellphone Is Keeping Tabs*, N.Y. TIMES, Dec. 21, 2003, at 1 (describing cellular phone services that allow customers to locate family members

Users of the available technology rely significantly upon public records made available by FOIL: "The power of web data collection, tracking, ad presentation, and similar technologies, combined with other traditionally public record data sources (and voter registration roles are just the tip of the iceberg) creates a scenario that might cause Darth Vader to be jealous."[50]

[18] According to Professor Davis, "The second major source of difficulties…is the routine presence of computers and the Web in work settings, and increasingly in households as well. Technology found only in research laboratories not long ago is now a widely available consumer product."[51] With the spread of personal computers in the home and at work, most of the teen and adult population of the country can access Web data through search engines twenty four hours a day, seven days a week.[52] "One consequence is that individuals routinely have the means and opportunity to access and copy vast amounts of digital information…but lack a clear picture of what is legal or ethically acceptable."[53]

[19] Nevertheless, state and local government executives and managers are under increasing pressure to develop and enhance e-government capabilities. E-government describes access to and the delivery of information and services by government online by digital means, primarily using the internet.[54] Many, if not most, state and local governments are

though global positioning technology; thus, indicating the reality of what Gerstner predicts is arriving).

[50] Lauren Weinstein, *Web Tracking and Data Matching Hit the Campaign Trail*, 8 PRIVACY FORM DIGEST 22 (1999), http://www.vortex.com/privacy/priv.08.22 (writing about presidential candidate ad buys in December, 1999).

[51] Davis, *supra* note 46, at 79.

[52] *See* John Markoff, *Internet Use Said to Cut Into TV Viewing and Socializing*, N.Y. TIMES, Dec. 30, 2004, at C5 (describing the results of a study that found approximately 75 percent of the population of the United States is estimated to have access to the Internet either at home or at work).

[53] Davis, *supra* note 46, at 79. Although the observation is made in the context of intellectual property, it is equally applicable to personally identifiable information.

[54] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (codified in scattered sections of 44 U.S.C.); *see also* ORG. FOR ECON. CO-OPERATION AND DEV., THE E-GOVERNMENT IMPERATIVE 23 (2003) (defining e-government as "equated to the use of ICTs [information and communications technologies] in government. While the focus is

placing policies, publications and databases online and are delivering government services online for residents.[55]

[20] Some of the reasons for the move to online information and services are well intentioned and similar to those of private business; they include lowering transaction costs and improving "customer" relations.[56] Pressures to improve administration and service delivery, particularly at times of fiscal retrenchment, have led to the development of and increased reliance upon electronic databases and automated systems. Agency heads are seeking to reduce mail transactions and visits to offices, both of which require greater amounts of personnel and space. Budget savings are potentially very significant:

> Movement from paper-based to web-based processing of documents and payments typically generates administrative cost savings of roughly 50 percent–more for highly complex transactions. This figure ignores additional savings of money, time, travel, and effort to citizens and intermediate institutions….The sheer volume of government transactions suggests the enormous savings electronic transaction processing alone could provide.[57]

generally on the delivery of services and processing, the broadest definition encompasses all aspects of government activity").

[55] GOLDSMITH & EGGERS, *supra* note 19, at 18-19.

[56] O'LOONEY, *supra* note 20, at 4, 23-24.

[57] FOUNTAIN, *supra* note 20, at 5; s*ee also* Stacy Albin, *Albany: License Renewal Goes Online*, N.Y. TIMES, Aug. 22, 2003, at B5 (renewing drivers' licenses online, by N.Y.S. Dept. of Motor Vehicles, with a receipt printed on a home computer serving as a temporary license); Micheline Maynard, *Will This Idea Fly? Charge Some Travelers $10 for Showing Up*, N.Y. TIMES, Aug. 25, 2004, at C1 (describing a cutting edge example, from the private sector, being implemented from Northwest Airlines, in charging an extra ten dollar fee for tickets issued at airports, a five-dollar fee for tickets purchased by telephone over its reservation lines, and leaving purchases through the airline's web site as the only way to avoid the fee); Bob Tedeschi, *Airlines, Needing to Cut Costs, Urge Travel Agents to Switch to a Web-Based Reservation System*, N.Y. TIMES, Jan. 31, 2005, at C4 (explaining how airlines are encouraging travel agents to shift from mainframe systems to web-based reservation systems, in part, because Web-based systems cost airlines about one dollar for every ticket booked in contrast to more than ten dollars per ticket with mainframe systems).

The use of private contractors to provide some government services expands the scope of those with access to and control over government information.[58] Computer and communications technologies have made it easier and cheaper for governments to use partners outside of government,[59] and state and local governments are increasingly using private partners.[60]

[21] In addition, the desire by residents to conduct transactions with government agencies over the Internet, a reflection both of convenience and of developments in the private sector,[61] requires electronic access to databases. "A[s] the Internet has grown up and consumers have become accustomed to going online for everything from banking to buying movie tickets, cities large and small have joined in by making more municipal services available on the Web."[62] In the public arena, in contrast to the private sector, failure to implement e-government services can have adverse political consequences for elected executive branch officials, particularly when the private sector and other governments are doing so.[63]

---

[58] An example is the Connecticut vehicle emissions testing program, which provides the contractor–Agbar Technologies–with online access to information about vehicle registrations. *See, e.g.*, William Yardley, *Emission Tests Will Resume After a Six-Month Suspension*, N.Y. TIMES, Oct. 9, 2004, at B6 (reporting restart of the Connecticut vehicle emissions testing program following a six-month shutdown by the state because of contractor software problems); JAMES J. FAZZALARO, OFFICE OF LEGISLATIVE RESEARCH, MOTOR VEHICLE EMISSIONS INSPECTION PROGRAM (2004), *available at* http://www.cga.ct.gov/2004/rpt/2004-R-0669.htm (analyzing difficulties with operation of emissions testing program and options). Once again, the information privacy goals of the Drivers Privacy Protection Act of 1994 are vitiated. *See infra* notes 153-163 and accompanying text; s*ee also* Metzger, *supra* note 19, at 1370 (questioning whether delegations of authority to private entities are adequately structured to enforce constitutional constraints on government power).

[59] GOLDSMITH & EGGER, *supra* note 19, at 17.

[60] *Id.* at 11 (noting that state government contracts with private firms increased by 65 percent during the five-year period between 1996 and 2001).

[61] GERSTNER, *supra* note 20, at 165-175 (describing IBM's new focus on e-business as a central theme of its new business model).

[62] Thomas J. Fitzgerald, *Service Is a Struggle For Virtual Town Halls*, N.Y. TIMES, Sept. 25, 2003, at G5; *see also* Neil Vigdor, *Snagged by the Web: Town Boosts Services on Internet Site*, GREENWICH TIME, Aug. 6, 2004, at A1 (reporting on increased service provided by Town of Greenwich online, with the town's information technology director touting idea of a virtual Town Hall, with "[t]wenty-four seven government").

[63] *See, e.g.*, Ronald Smothers, *Governor Says The Problems With E-ZPass Are Solved*, N.Y. TIMES, July 13, 2004, at B5 (describing political backlash following New Jersey's difficulties in implementing E-ZPass on the State's highways); *see also* Vigdor, *supra*

[22] A brief look at three databases–voter registration, geographic information system (GIS),[64] and recreation management–used by many local governments illuminates the issues. All three are in use by Greenwich, Connecticut, a medium-size Connecticut town (population approximately 62,000)[65] recently involved in FOIL litigation regarding its GIS system.[66] The town's voter registration system includes the following information for 38,000 registered voters: name, address, date of birth, and political party affiliation.[67] A key element from the privacy standpoint is the inclusion of residents' dates of birth.

[23] The GIS includes the following information for each property in the town: address, property ownership, aerial digital photographs, and the location of roads, utility, fiber optic networks, and sewer lines.[68] Invoking the Connecticut FOIA, a self-employed computer consultant requested a copy of "the GIS database backup tapes," including "orthophotography,[69] arc info coverages,[70] SQL server databases[71] referenced to GIS data, and

note 62, at A1 (Greenwich first selectman describing Town web services as "essential for communicating with constituents" and saying "they're now must haves").

[64] "GIS is a computer system capable of assembling, storing, manipulating, and displaying geographically referenced information that may by used to make multifaceted interrelationships among many types of data visually intelligible." County of Suffolk v. First Am. Real Estate Solutions, 261 F.3d 179, 186 n. 4 (2d Cir. 2001).

[65] U.S. Census Bureau (2002), http://www.census.gov/popest/cities/tables/SUB-EST2003-05-09.pdf.

[66] *See infra* notes 68-93 and accompanying text.

[67] E-mail from Laurence Simon, Member of Town of Greenwich Board of Estimate and Taxation, to Ira Bloom, author (Oct. 26, 2005) (on file with author); *see also infra* note 105.

[68] Whitaker v. Dir. Dep't of Info. Tech., No. FIC2001-546 (F.I.C. C.T. 2002), *available at* http://www.state.ct.us/foi/2002FD/20021113/FIC2001-546.htm.

[69] Orthophotography is defined as "digital imagery in which distortion from the camera angle and topography have been removed, thus equalizing the distances represented on the image." GIS Lounge, Glossary, http://gislounge.com/glossary/bldeforthophotography.shtml (last visited Jan. 23, 2006).

[70] ArcInfo coverages are created from sources such as paper maps and photographs, which then must be converted through a series of steps to digital form. University of California Davis, Review of Understanding GIS – the ARC/INFO Method, http://ice.ucdavis.edu/local/gis/arctut4.html (last visited Jan. 23, 2006).

[71] SQL refers to Structured Query language, "a standard language used to formulate queries posed to databases." Martin Libiicki Et Al., SCAFFOLDING THE NEW WEB: STANDARDS AND STANDARDS POLICY FOR THE DIGITAL ECONOMY xxii (2000).

all documentation created to support/define coverages,"[72] essentially all of the town of Greenwich's computer data used in connection with its GIS system. The consultant declined the town's offer to provide him with printed maps.[73] He stated that he intended to use the GIS data to market and sell various services, which may involve posting the data on the internet.[74] The town denied the FOIA request and the consultant then appealed to the Connecticut Freedom of Information Commission, which ordered the town to provide the requested information.[75] The town thereafter appealed the Commission's decision to the Superior Court, which affirmed the decision of the Commission.[76] The town, in turn,

[72] Brief for the Plaintiff at 2, Director Department of Information Technology v. Freedom of Information Commission & Stephen Whitaker, No. CV 03 0519153-S (Aug. 6, 2003) [hereinafter Brief for the Plaintiff] (on file with author).

[73] Whitaker v. Dir. Dep't of Info. Tech., No. FIC2001-546 (F.I.C. C.T. 2002) (illustrating the value of digital, as opposed to analog, data); *see* Davis, *supra* note 46 and accompanying text. If the consultant's purpose were to evaluate the Town's governmental operations, printed maps would serve the purpose. Mr. Whitaker, however, claimed "I can't do any analysis from a paper map." Neil Vigdor, *Town Raising Prices for GIS Aerial Photos*, GREENWICH TIME, Nov. 19, 2004, at A1 (reporting upon increased price charged by Town of Greenwich for GIS aerial property photos). Although one expert has noted that analog data can be scanned, there would be considerable difficulty and potential for considerable deterioration of data in scanning all of the data in so large a file. Denise G. Callahan, *Internet Access to Court Documents Is Creating Privacy Problems*, LAWYERS WEEKLY USA, Mar. 28, 2005 (quoting Jim McMillan, Director, Court Technology Laboratory, National Center for State Courts).

[74] Neil Vigdor, *GIS Data Could Go Public: Town Plans to Fight FOI Officer's Findings on Access*, GREENWICH TIME, Oct. 25, 2002, at A1.

[75] Whitaker v. Dir. Dep't of Info. Tech., No. FIC2001-546 (F.I.C. C.T. 2002)

[76] *See* Vigdor, *GIS Data Could Go Public*, *supra* note 74, at A1; Neil Vigdor, *Town Loses Public-Records Case*, GREENWICH TIME, Jan. 6, 2004, at A1 (reporting decision by Superior Court Judge Harold Owens Jr.). Greenwich, often described in the media as an affluent town, is the home of many senior corporate executives and celebrities. *See, e.g.*, Berner, *supra* note 27, at 144; Hugh Eakin, *Greenwich Gets a Renaissance All Its Own*, N.Y. TIMES, Jan. 30, 2005, at 38 AR (reporting changes made by a new Director at the Town's Bruce Museum of Art and Science, while describing Greenwich as an affluent community "which is better known for its coveted suburban real estate than for exhibitions of art" and stating that the Director has "proved adept at connecting with his well-heeled Greenwich base"); Alison Leigh Cowan, *Millionaires Made of Steel May Avoid An Old Tax*, N.Y. TIMES, Mar. 26, 2006, at 3 CT (reporting upon potential impact of Connecticut Governor's proposal to repeal Connecticut personal property tax on automobiles, but emphasizing number of very high priced cars registered in Town of Greenwich).

appealed the decisions to the Connecticut Court of Appeals.[77] The Connecticut Supreme Court, however, decided to hear the appeal, bypassing the Court of Appeals.[78] The case achieved national attention, with three groups–the Reporters Committee for Freedom of the Press, the Society of Environmental Journalists, and Investigative Reporters and Editors, Inc.–filing an amicus brief in support of the Commission and Mr. Whitaker.[79]

[24] On June 21, 2005, the Connecticut Supreme Court released its June 15th unanimous decision.[80] The court emphasized the FOIA statutory policy which favors disclosure, explaining that "any exception to that rule will be narrowly construed in light of the general policy of openness expressed in the [act]."[81] The standard of review appropriate in applying the meaning of the exemptions is "whether the commission's factual determinations are reasonably supported by substantial evidence in the record taken as a whole."[82]

[25] The Connecticut Supreme Court rejected several principal arguments put forward by the town. In response to the contention that the GIS was

[77] Ivan H. Golden, *Appeal Planned on GIS Decision*, GREENWICH TIME, Jan. 10, 2004, at A1 (reporting decision of the town to appeal Superior Court decision); Neil Vigdor, *Town Seeks Visual Appeal*, GREENWICH TIME, July 31, 2004, at A1 (reporting the town's attempt to make visual demonstration of its GIS before Connecticut Court of Appeals).
[78] Neil Vigdor, *Supreme Review: State's Highest Court to Hear Town Case on Public Records*, GREENWICH TIME, Sept. 22, 2004, at A1 (reporting that Connecticut Supreme Court decided to hear the case, leap-frogging the Court of Appeals); Ivan H. Golden, *State's Highest Court to Hear GIS Case Jan. 6*, GREENWICH TIME, Dec. 21, 2004, at A3 (reporting that Supreme Court scheduled oral arguments for Jan. 6, 2005).
[79] Ivan H. Golden, *GIS Case Gains National Attention*, GREENWICH TIME, Oct. 22, 2004, at A1; Ivan H. Golden, *News Groups Back Release of Town Data*, GREENWICH TIME, Nov. 10, 2004, at A1(reporting comments by several organizations and academics).
[80] Dir., Dep't of Info. Tech. v. Freedom of Info. Comm'n, 874 A.2d 785 (Conn. 2005) (affirming order to release Town of Greenwich GIS database in electronic format in response to request under Connecticut Freedom of Information Act, two justices not participating in the decision); Neil Vigdor, *Town Ordered to Give Up Records*, GREENWICH TIME, June 16, 2005, at A1 (reporting Connecticut Supreme Court decision ordering release of GIS database).
[81] *Dir., Dep't of Info. Tech.*, 874 A.2d at 791 (quoting Ottochian v. Freedom of Info. Comm'n, 604 A.2d 351 (Conn. 1992)) (internal citations omitted).
[82] *Id.* (quoting Rocque v. Freedom of Info. Comm'n, 774 A.2d 957 (Conn. 2001)) (internal citations omitted).

entitled to exemption from disclosure as a trade secret,[83] the court found that because the GIS data is readily available to the public it did not fall within the trade secret exemption:

> Members of the public seeking the GIS data could obtain separate portions of the data from various town departments, where that data is available for disclosure. The requested GIS database *simply is a convenient compilation of information that is already available to the public.* The records therefore fail to meet the threshold test for trade secrets, that the information is not generally ascertainable by others.[84]

The court's rationale ignores the significance of the electronic database both for purposes of resolving the trade secret issue and more generally. The database is more than a convenient compilation of information that is already available to the public in analog form. Releasing "the GIS database backup tapes including orthophotography, arc info coverages, SQL server databases referenced to GIS data, and all documentation created to support/define coverages"[85] enables the recipient to utilize the system itself, not just the information included in the system. The court fails to distinguish between the information held within the system and the system itself, which is the trade secret. The release of the backup tapes also enables the recipient to manipulate, mine, and transfer the data, as well as to merge the data with other databases.[86] As already noted, the impact of digital compilations upon privacy and security can be extraordinary, particularly if, as suggested at one point by the requestor in this case, the data may be placed on the Internet.[87] The consequences of technological inversion are ignored by the court.

[26] The court also rejected the town's arguments involving both physical safety and information security. The court concluded that the Police Chief's testimony was insufficient to establish that the release of the GIS

[83] CONN. GEN. STAT. § 1-210(b)(5)(A)(2004).
[84] *Dir., Dept. of Info. Tech*., 874 A.2d at 795 (emphasis added).
[85] Brief for the Plaintiff, *supra* note 72, at 2; *see supra* notes 69-72 and accompanying text for definitions of these terms.
[86] *See supra* notes 24-26 and accompanying text.
[87] Brief for the Plaintiff, *supra* note 72, at 3. *See supra* note 25 and accompanying text.

data would pose a safety risk for the town or its residents.[88] The court supported the trial court's suggestion that statistical data correlating criminal or terrorist activity with the disclosure of GIS data would have been helpful in establishing the risks.[89] It is difficult to see, however, how the statistics could be amassed until after the GIS database is released, and then, of course, the damage would be done. The court also rejected as insufficient the testimony of the town's Director of Information Technology, presumably expert testimony, that the release of the GIS database would compromise the security and integrity of the town's information technology system.[90]

[27] Finally, the court faulted the town for failing at an earlier stage of the case to avail itself of a 2002 amendment to the Connecticut FOIA which amended exemption nineteen, involving safety risks, by adding a procedure for consultation with the Commissioner of Public Works.[91] "The plaintiff never sought the required consultation with the commissioner of public works. Nor did he at any time request that the trial court remand the case so that the public works commissioner could make a public safety determination."[92]

[28] Although there are several statements in the opinion noting the town's failure to invoke available procedures and possible failures of proof, the court itself, nevertheless, is responsible for the troublesome aspects of the opinion. The court fails to recognize the consequences to public policy of the migration of public records to digital databases. Further, as in *Davis v. Freedom of Information Commission,*[93] a case involving the Drivers Privacy Protection Act, the court almost blindly

[88] *Dir., Dept. of Info. Tech.*, 874 A.2d at 793.
[89] *Id.*
[90] *Id.* at 795; *see* CONN. GEN. STAT. § 1-210(b)(20)(2004).
[91] *Dir., Dept. of Info. Tech.*, 874 A.2d at 791; *see* CONN. GEN. STAT. § 1-210(b)(19)(A)(2004); *see infra* note 142 and accompanying text.
[92] *Dir., Dept. of Info. Tech.*, 874 A.2d at 792. Following the decision the dispute continued, with Whittaker complaining before the Connecticut Freedom of Information Commission that the Town is withholding some of the data. Following a decision by the Commissioner of Public Works, the Town removed a few "layers of data" showing locations of fire hydrants, manholes, storm drains, and utility poles. Kenneth Partridge, *GIS fight continues*, Greenwich Post, Dec. 1, 2005, at 1A *and* Brian Lockhart, *FOI Commission is 'agency of the people,'* GREENWICH TIME, Mar. 16, 2006, at A1.
[93] Davis v. Freedom of Info. Comm'n, 790 A.2d 1188 (Conn. Super. Ct. 2001); *see infra* notes 157-160 and accompanying text.

supports the most far-reaching interpretation of the FOIA without giving adequate weight to countervailing legal and policy considerations.

[29] The seemingly benign department in town government–the Department of Parks and Recreation–maintains and uses a recreation management system database for issuing park passes, tennis permits, golf permits, and registering participants for most of the Town's recreation programs.[94] At present, under the current interpretations of Connecticut's FOIL, all three of these databases (voter registration, GIS, and recreation management) can be requested under FOIL in electronic format and likely would have to be made available. The three databases are not the only ones used by the town of Greenwich. Others include real and personal (boats and cars) property tax assessments,[95] library card holders,[96] and holders of railroad parking stickers,[97] an important matter in a town with a significant number of commuters.

[30] As is typical, the town does not have any central review or policymaking forum that addresses how electronic databases with personally identifiable information are managed.[98] Furthermore, a larger

[94] The system in use is RecTrac. Vermont Systems, RecTrac, http://www.vermontsystems.com/scripts/vsiweb.wsc/rectrac.htm?xxpref=RT (last visited Feb. 6, 2006) (providing descriptions of the components and capabilities of the RecTrac system); see also Fitness Solutions, RecTrac, http://leisuresolutions.sportingpulse.com/index.php?id=12 (last visited Feb. 6, 2006).

[95] *See infra* notes 155-160 and accompanying text.

[96] Librarians are concerned about requests by law enforcement officials for information about reading material and other internal matters, reporting over 200 formal and informal inquiries made to libraries since October 2001. Eric Lichtblau, *Libraries Say Yes, Officials Do Quiz Them About Users*, N.Y. TIMES, June 20, 2005, at A11. Even the technology increasingly used by libraries to "check out" books is becoming controversial. Many university libraries are beginning to implement radio frequency identification (RFID), which uses an embedded electronic product code (EPC), a unique identifier. The RFID tags, which can be read through a bag or coat, allow considerable data to be stored, such as the names of prior borrowers and their addresses. *See* Paul Rubell, *Wireless World: Libraries' Use of RFID Tags Spurs Privacy, Legal Concerns*, N.Y.L.J., Aug. 24, 2004, at 5; *see also infra* note 244 regarding library records and USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001).

[97] E-mail from Larry Simon, Member of Greenwich Board of Estimate and Taxation, to Ira Bloom, Professor of Political Science, Lehman College, City University of New York (Oct. 26, 2005, 06:24:00 EST) (on file with author).

[98] *See id.* A survey conducted in the year 2000 revealed that only five percent of government websites showed some form of security policy and only seven percent had a

population of the municipality results in a greater size and number of databases in use.

[32] Information in different databases can be cross-matched, making a valuable and potentially damaging trove of personal information about residents and families available to the public under FOILs. Cross-matching, by using the resident's address, for example, as the common data element–a relatively easy task–would yield at low cost information which can be used for commercial or malevolent purposes.[99]

B. POSTING DATABASES ON THE INTERNET

[33] As noted, a significant aspect of e-government is communication and activity using the Internet.[100] Most state and local governments, even small jurisdictions, are placing policies, publications, and databases online and are greatly expanding the delivery of government services online for residents.[101] In the aftermath of the events of September 11, 2001, states and municipalities would be wise to establish policies for posting information and to rethink some of the web postings,[102] particularly those potentially involving the lives and safety of their residents, including, for example, the location of key infrastructure systems.[103] By contrast, at the

privacy policy. Darrell M. West, *Assessing E-Government: The Internet, Democracy, and Service Delivery by State and Federal Governments*, Sept., 2000, http://www.insidepolitics.org/egovtreport00.html; *see infra* note 105 and accompanying text.

[99] Information in state and local databases can also be combined with other sources of information about residents. A news report, whose source was the Center for Responsive Politics, reported upon campaign contributions to 527 groups ranging up to $500,000 by twenty Greenwich residents. Such data provide a strong indicator of individual wealth. Neil Vigdor, *Greenwich's Deep Pockets Bankroll '527' Groups*, GREENWICH TIME, Oct. 31, 2004, at A1 (reporting on Greenwich donors and 527s receiving the most money from Greenwich).

[100] *See supra* notes 54-55 and accompanying text.

[101] *See supra* note 62-63 and accompanying text.

[102] Even prior to September 11, the International City/County Management Association (ICMA) cautioned: "When information is available over the Internet, such informal checks [practical obscurity] on data gathering no longer exist." O'LOONEY, *supra* note 20, at 92. See also note 20 and accompanying text.

[103] The issue of public safety considerations as a basis for denial of a FOIA request, which possibly would lead to Internet posting, was raised by the town of Greenwich and rejected by the CT Freedom of Information Commission in the GIS case. Whitaker v. Dir. Dep't of Info. Tech., No. FIC2001-546 (F.I.C. C.T. 2002), *available at*

federal level the Homeland Security Act added a new Federal FOIA exemption for critical infrastructure.[104]

[34] Quite troubling, however, is that, even within local governments, decisions regarding the posting of information on agency internet web sites are often decentralized and are subject to limited oversight and control by elected officials, often surprising residents and their elected representatives.[105] Once online, of course, all of the material is available

---

http://www.state.ct.us/foi/2002FD/20021113/FIC2001-546.htm. The town is using the GIS as a key element in its planning for emergency operations. Martin B. Cassidy, *Town's Digital Database Gets New Emergency Role,* GREENWICH TIME, Aug. 6, 2004, at A3 (reporting that the GIS will be used to produce maps showing locations of fire hydrants, police cars, and fire trucks during emergencies). The consequences of the 2002 amendment of exemption nineteen of the Connecticut FOIA are unclear. With the Connecticut Supreme Court's continuing emphasis upon construing exemptions narrowly (see *supra* note 81 and accompanying text), it is not certain what degree of deference will be given to the findings of the Commissioner of Public Works. *See supra* notes 91-92 and accompanying text; *infra* note 142 and accompanying text.

[104] The Federal Government moved after September 11 to restrict access to critical infrastructure information, an action which was codified in the Critical Infrastructure Information Act of 2002, 6 U.S.C. § 133(a)(1), (a)(1)(A) (2000), through the creation of an exemption to the Federal FOIA. Although subject to criticism within Congress and by some FOIL advocates, the change is a rational response to current threats. *See* Kristen Elizabeth Uhl, Comment, *The Freedom of Information Act Post 9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security,* 53 AM. U. L. REV. 261, 294, 296, 302-03 (2003).

[105] *See, e.g.*, Amy Harmon, *As Public Records Go Online, Some Say They're Too Public,* N.Y. TIMES, Aug. 24, 2001, at A1 (reporting upon new web site making New York City voter registration records, including home addresses, available on the web); Bruce Lambert, *Online Trove of Property Data Is Raising Concerns in Nassau,* N.Y. TIMES, Sept. 27, 2002, at B6 (reporting upon the decision of the Chairman of the Nassau County Board of Assessors to place property data for every home and business, including color photographs, on the web and the reactions to this action); Jennifer Lee, *Dirty Laundry, Online for All to See,* N.Y. TIMES, Sept. 5, 2002, at G1 (describing decision of the clerk of courts for Hamilton County, Ohio to post county court records–including state tax liens, arrest warrants, bond postings, traffic infractions, etc–much to the chagrin of many residents); Joyce Purnick, *A Homeowner And a Taste of Bureaucracy,* N.Y. Times, Feb. 20, 2006, at B1 (describing difficulty of removing unfounded complaints from website of New York City Dept. Of Buildings).

Court systems are one of the few venues in which these issues have been publicly debated. Court systems have been addressing the issue of whether court filings should be made available electronically over the internet and the concomitant privacy issues. *See, e.g., Rules Change to Protect Privacy,* THE THIRD BRANCH (Admin. Office of the U.S. Courts, Washington, D.C.), Dec. 2003, at 7, *available at*

http://www.uscourts.gov/ttb/dec03ttb/privacy/index.html (describing changes to Federal Rules of Bankruptcy Procedure–Rules 1005, 1007, and 2002–requiring that cases no longer display filer's entire social security number when case is viewed electronically); *Electronic Access Available to Criminal Case Files*, THE THIRD BRANCH (Admin. Office of the U.S. Courts, Washington, D.C.), Oct. 2004, at 5, *available at* http://www.uscourts.gov/ttb/oct04ttb/access/index.html (announcing that beginning Nov. 1, 2004, federal criminal case file documents will also be available remotely through electronic access, but "[a]s with civil and bankruptcy cases, personal data identifiers [including social security and financial account numbers to the last four digits, dates of birth to the year, and home addresses to the city and state] must be redacted by the filer of a criminal case document, whether the document is filed electronically or in paper"). Some states, including Florida and Ohio, however, are backing away from online access to court records because of privacy concerns. Callahan, *supra* note 73, at 6. The public outcry in response to the Hamilton County clerk of courts actions, noted above, was in part responsible for the Ohio Supreme Court policy review. The clerk of courts' actions also resulted in a December 2004 Federal lawsuit against the County, alleging that information available on the website led to identity theft. *Id.*

For an informative discussion of the movement to internet access to court documents in the Federal judiciary and in the New York State Court system, see Arminda Bradford Bepko, *Public Availability or Practical Obscurity: The Debate Over Public Access to Court Records on the Internet*, 49 N.Y.L. SCH. L. REV. 967 (2005). The author's conclusion, however, that "[t]he First Amendment right to inspect court documents should be extended from the courthouse onto the internet regardless of the information contained within those documents," is based upon faulty premises–including the failure to recognize the threat to privacy and to information safety posed by the postings, as well as the purported "voluntary" decision by a litigant to place personal information in court records. Indeed, an argument can be made that these actions threaten a person's Constitutional right of access to the courts. *Id.* at 982-983, 990.

The Executive Branch of the Federal Government is recognizing some of these privacy concerns. On September 26, 2003, the Office of Management and Budget (OMB) issued guidance on implementing privacy provisions of the E-Government Act of 2002. OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB MEM. NO. 03-22, OMB GUIDANCE FOR IMPLEMENTING THE PRIVACY PROVISIONS OF THE E-GOVERNMENT ACT OF 2002 (2003), *available at* http://www.whitehouse.gov/omb/memoranda/m03-22.html (providing regulations for The E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2889 (codified in scattered sections of the United States Code)). In accordance with the guidelines, agencies are directed to conduct Privacy Impact Assessments (PIAs) on information technology systems. Among other issues, the PIAs are to analyze why the information is being collected, the parties with whom the information will be shared, and what opportunities people will have to decline to provide the information or to consent to particular uses. *See OMB Issues Guidance on Implementing Privacy Provisions of E-Government Act,* U.S. L. WK., Oct. 7, 2003, at 2188-2189.

to anyone, anywhere, with internet access, seven days a week, twenty-four hours a day.[106] Web posting decisions are also controversial even among some FOIL advocates. Interestingly, the Director of the New York State Committee on Open Government, a passionate advocate of public disclosure, questioned the "wisdom of putting . . . [the Nassau County assessments] up on a Web site for all to see."[107] This point of view is challenged, however, by other proponents of open records, including Charles Davis, executive director of the Freedom of Information Center at the Missouri School of Journalism, stating, "The greatest tool in the history of mankind toward promoting access is being turned into this demonic force for the invasion of privacy. We're equating ease of access with privacy, and to me they're two different animals. Either a record is private or it's not."[108]

[35] The extensive use of large databases with personally identifiable information and their ease of manipulation also require the exercise of great care by public employees. The possibility of inadvertently posting confidential records is an ever present threat, as illustrated by the experience of a school district in the State of Washington, which accidentally posted almost 7,000 confidential student records on its public internet website.[109] In addition, what is made available may be more than

[106] The security risks of posting were demonstrated by the discovery by U.S. military forces in Iraq of diagrams and photographs of public schools in several states that had evidently been downloaded from government Web sites. Eric Lichtblau, *Iraq Disk Mentions U.S. Schools*, N.Y. TIMES, Oct. 8, 2004, at A18; Sean Cavanagh & Kathleen Kennedy Manzo, *Districts Rethink Availability of Data on School Security*, EDUC. WK., Oct. 20, 2004, at 18 (reporting upon discussions among school administrators about limiting access to school information on the internet following F.B.I. warnings and including copy of floor plans of a Pennsylvania elementary school found on the internet).

[107] Lambert, *supra* note 105. Nevertheless, the Committee ruled against neighboring Suffolk County's attempt to copyright its GIS system. County of Suffolk v. First Am. Real Estate Solutions, 261 F.3d 179 (2d Cir. 2001); *see also infra* notes 256-272 and accompanying text.

[108] Harmon, *supra* note 105. The simplistic view that records are either public or private is considered in Section IV.B.2. *See infra* notes 198-201 and accompanying text.

[109] Andrew Trotter, *Confidential Records Mistakenly Posted on the Internet*, EDUC. WK., Oct. 8, 2003, at 5 (reporting that records for all 6,916 students in grades 5-8 in Vancouver, Wash. School District were accidentally placed on District's public web site). Privacy of student records is protected by the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2000). *See infra* note 178 and accompanying text; *see also Error on Student Warnings*, N.Y. TIMES, June 19, 2005, at 20 (reporting error made by Office of Financial Aid of the University of Kansas in which individual e-mail messages

intended because of technical and programming mistakes by information technology staff.[110]

[36] Security of governmental databases and concomitant unintentional disclosure of information as a consequence of hacking and other threats are additional concerns.[111] In a rare example of attention to security breaches and in recognition of risks–including identity theft–created by widespread collection of personal information in the public and private sectors, California now requires that state agencies disclose breaches of security that lead to unauthorized access to personal information about California residents.[112]

III. FOILS AND THE AVAILABILITY OF DIGITAL INFORMATION: CREATING THE PROBLEM

[37] All fifty states have enacted FOILs, many doing so after the Federal Freedom of Information Act[113] was enacted in 1966.[114] A large majority of the state FOILs follow the open records approach of the federal

sent to 119 students were inadvertently sent to all, enabling each of the recipients to see the names of all of the students receiving the message).

[110] *See, e.g.*, Yuki Noguchi, *Online Search Engines Lift Cover of Privacy*, WASH. POST, Feb. 9, 2004, at 6 (describing how confidential data can turn up through internet search engines because of improperly configured servers, holes in security systems, and human error on the part of the entity holding the information).

[111] *See, e.g.*, ASSEMBLYMAN JEFF KLEIN, CHAIR, NYS ASSEMBLY COMMITTEE ON OVERSIGHT, ANALYSIS AND INVESTIGATION, ANNUAL 2003 REPORT 9-11 (2003), http://assembly.state.ny.us/comm/Oversight/2003Annual (reporting upon lack of attention to information security by New York State agencies); Ellen Perlman, *Breaking and Entering*, CQ/GOVERNING, Oct. 2004, at 16 (describing the difficulties faced by state and local officials seeking to secure their networks).

[112] CAL. CIV. CODE § 1798.29 (West 2004). CAL. CIV. CODE § 1798.82 (West 2004) applies similar requirements to people or businesses that conduct business in California. This statute recently forced a number to companies–including ChoicePoint, LexisNexis, Wachovia, and Ameritrade–to reveal substantial data security breaches. Tom Zeller, Jr., *The Scramble to Protect Personal Data*, N.Y. TIMES, June 9, 2005, at C1.

[113] Freedom of Information Act, 5 U.S.C. § 552 (2000). Twenty two additional states, including New York, added data breach laws during 2005. Freedman, *supra* note 7. For discussions of the New York State Information Security Breach and Notification Act, effective Dec. 7, 2005, *see* Mark G. Milone, *Information Insecurity*, N.Y. L.J., Oct. 25, 2005, at 5; Stephen V, Treglia, *I.D. Theft Notification*, N.Y. L.J., Nov. 15, 2005, at 5; Yair Y. Galil & Mauricio F. Paez, *Strict Requirements, Harsh Penalties Mark State's New Data Breach Act*, N.Y. L.J., Jan. 30, 2006, at S7.

[114] Nowadzky, *supra* note 11, at 65.

statute.[115] A standard public administration text describes the purpose of FOILs:

> Holding government officials accountable for their actions and conduct is crucial to democratic government, even more so when substantial responsibility is entrusted to nonelected (administrative) personnel. This rationale underlies the need for openness in government operations, public scrutiny, and freedom of information (FOI) and sunshine laws, all of which increase the public's ability to inquire successfully into the activities of bureaucracy and other branches of government.[116]

The Federal FOIA includes an explicit exemption, exemption six, for "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[117]

[38] The New York and Connecticut FOILs are typical of the state FOILs in their scope and coverage.[118] They differ from each other markedly, however, in some key aspects.

A. NEW YORK STATE

[39] The New York State Freedom of Information Law–Article 6 of the Public Officers Law–was initially adopted in 1974.[119] It declares: "The people's right to know the *process of governmental decision-making* and to review the documents and statistics *leading to determinations* is basic to our society. Access to *such* information should not be thwarted by shrouding it with the cloak of secrecy or confidentiality."[120] The New

[115] *Id.* at 65-66.
[116] MICHAEL E. MILAKOVICH & GEORGE J. GORDON, PUBLIC ADMINISTRATION IN AMERICA 51 (2001).
[117] 5 U.S.C. § 552(b)(6) (2000). *See also* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 35-56 (1973). For a comprehensive summary of the legislative history and application of this provision, *see generally* LITIGATION UNDER THE FEDERAL OPEN GOVERNMENT LAWS 125-161 (Harry A. Hammitt et al. eds., 2002).
[118] *See* Nowadzky, *supra* note 11, at 66 n.6.
[119] N.Y. PUB. OFF. LAW §§ 84-90 (McKinney 2004).
[120] *Id.* § 84 (emphasis added).

York FOIL also includes a provision seeking to prevent "unwarranted invasions of personal privacy," which provides for "deletion of identifying details or withholding of records otherwise available."[121] An unwarranted invasion of personal privacy includes, but is not limited to, six circumstances, including "sale or release of lists of names and addresses if such lists would be used for commercial or fund-raising purposes."[122] As with other FOILs, the New York State courts have ruled that the FOIL is to be construed liberally and its exemptions interpreted narrowly.[123]

[40] New York state law includes two statutory provisions designed to protect the interests of people about whom New York State agencies have collected information: Article 6-A of the Public Officers Law–the Personal Privacy Protection Law[124]–and Article II of the State Technology Law–the Internet Security and Privacy Act.[125] Both, however, include exceptions for requests made under the FOIL.[126]

[41] Notwithstanding the judiciary's emphasis on liberal construction of the statute and the narrow scope of the exemptions, a proper interpretation of the statute, when applied to agency-held databases, should lead to a greater protection of privacy. The emphasis in the legislative declaration upon documents "leading to determinations," combined with legislative concern manifested in the FOIL's unwarranted invasion of privacy provision, should lead to the conclusion that agency databases maintained for convenience in administering programs, such as recreation management systems, and elements of programs, such as the names of owners of properties in GIS records and social security numbers of voters in voter registration lists, should not be made available in response to FOIL requests. Increasingly, much of the information in these databases

[121] *Id.* § 89(2)(a).
[122] *Id.* § 89(2)(b)(iii).
[123] *See, e.g.*, Newsday, Inc. v. Sise, 518 N.E.2d 930, 932-33 (N.Y. 1987) (holding that records containing names and addresses of jurors exempted from disclosure by Judiciary Law); Prisoners' Legal Services v. N.Y.S. Dep't of Corr. Serv., 535 N.E.2d 243, 246 (N.Y. 1988) (holding that personnel records of corrections officers exempted from disclosure by Civil Rights Law § 50-a).
[124] N.Y. PUB. OFF. LAW §§ 91-99 (McKinney 2004).
[125] N.Y. STATE TECH. LAW §§ 201-207 (McKinney 2002).
[126] N.Y. PUB. OFF. LAW § 96(1)(c) (McKinney 2004) (exempting FOIL requests from the Personal Privacy Protection Law); NY. STATE TECH. § 207 (McKinney 2002) (exempting FOIL requests from the Internet Security and Privacy Act).

is maintained for convenience and efficiency in the administration of programs and is never presented to public officials for the purpose of making determinations of public policy. Consequently, the New York state courts should reexamine their decisions regarding the FOIL in the light of the intent of the statute and the technological inversion that has occurred.

[42] Perhaps surprisingly, the New York State Committee on Open Government, the agency charged with administering New York State's FOIL,[127] is recognizing cautiously the increasing importance of security and privacy issues since September 11, 2001, particularly as it affects the lives and safety of people. At the October 2003 Committee meeting, Robert Freeman, Executive Director of the Committee, "indicated that following Sept. 11 there is an increased need for security which has caused 'some variations on issues,' but that, 'in general . . . FOIL does not need to be amended in New York.'"[128]

[43] Even more surprising is the concern of the Committee regarding personal privacy issues, particularly as they encompass the Internet. The Committee acknowledged that the Internet poses "an additional problem by removing traditional barriers to obtaining information about individuals and underscoring the need for consideration before agencies post such information on web sites."[129] Executive Director Freeman cautioned: "Issues involving privacy are difficult and inconsistent . . . . In other words, you better think first."[130] Unfortunately, the concerns of the Committee do not yet appear to have significantly impacted either agency behavior or the Committee's own actions.[131]

---

[127] N.Y. PUB. OFF. LAW § 89(1)-(2) (McKinney 2004).
[128] Dakotah Pratt-Hewitt, *Open Government Group Seeks Amendment to Force Payments*, THE LEGISLATIVE GAZETTE, Oct. 20, 2003, at 2.
[129] *Id.*
[130] *Id.*
[131] *See* Lambert, *supra* note 105, and accompanying text. *See also* Investigation Tech. v. Horn, 4 Misc. 3d 1023A (N.Y. Sup. Ct. 2004) (supporting rejection by New York City of FOIL request for dates of birth of detainees–including many arrested but not convicted–held in New York City jails by web business that compiles criminal records for background checks). In *Investigation Technologies*, the Committee on Open Government gave insufficient weight to the unwarranted invasion of personal privacy provision, particularly the provision regarding release of lists for commercial purposes. *Id.*; N.Y. PUB. OFF. LAW § 89(2)(b)(iii) (Consol. 2005). Although there is considerable opinion

B. CONNECTICUT

[44] The Connecticut Freedom of Information Act (FOIA)[132] presents consequential differences from the New York FOIL.[133] Enacted initially in 1963 and lacking a statutory statement of purpose, the FOIA begins with a set of encompassing definitions.[134] It defines "public records or files" as "any recorded data or information relating to the conduct of the public's business prepared, owned, used, received or retained by a public agency . . . whether such data or information be handwritten, typed, tape-recorded, printed, photostated, photographed or recorded by any other method."[135] The Connecticut FOIA does not require the connection to official decision making invoked by the New York FOIL, and thus exposes more databases with personally identifiable information to public disclosure.[136]

[45] The Connecticut FOIA includes a lengthy set of twenty categories of exempt records,[137] which is nevertheless less protective of privacy than the New York FOIL exemptions.[138] The only reference to "disclosure . . . which would constitute an invasion of personal privacy"[139] is included in the second of the exemptions and is drafted in a narrow manner to refer to "personnel or medical files and similar files."[140] This reference also includes a provision, initially enacted in 1995 and since added to, providing for the nondisclosure of residential addresses of certain individuals, *inter alia*, judges and police officers.[141] In addition, a provision was amended in 2002 to extend the public safety exemption included in subsection nineteen.[142]

---

that the purpose of a FOIL request is irrelevant, *see, e.g.*, *In re* Capital Newspapers v. Burns, 67 N.Y. 2d 562, 567 (1986), in this instance, the statute itself makes it relevant.

[132] CONN. GEN. STAT. § 1-200 (2005).

[133] N.Y. PUB. OFF. LAW § 88 (Consol. 1999).

[134] CONN. GEN. STAT. § 1-200.

[135] CONN. GEN. STAT. § 1-200(5) (2005).

[136] *See* CONN. GEN. STAT. § 1-200; N.Y. PUB. O. LAW § 88 (Consol. 1999).

[137] CONN. GEN. STAT. § 1-210(b)(1)-(20) (2005).

[138] *See* N.Y. PUB. OFF. LAW § 88 (Consol. 1999).

[139] CONN. GEN. STAT. § 1-210(b)(2).

[140] *Id.*

[141] CONN. GEN. STAT. § 1-217(a) (2005).

[142] CONN. GEN. STAT. § 1-210(b)(19). Section 1-210(b)(19) provides, in pertinent part, for exemption from disclosure as follows:

[46] The FOIA fails to recognize the consequences of digital technology by explicitly providing that nonexempt records maintained in a "computer storage system" shall be provided to a requestor in the "electronic storage device or medium requested by the person."[143] A Freedom of Information Commission is established to administer the FOIA.[144]

[47] As in most states, the Connecticut courts have ruled that the "policy underlying the Freedom of Information Act (FOIA) favor[s] the disclosure of public records"[145] and that "any exception to that rule will be narrowly construed in light of the general policy of openness expressed in the [act]."[146] Nevertheless, there is at least one decision cautioning that a "balance" between governmental needs for privacy and the public's right to know must govern the application and interpretation of the FOIA.[147] It is significant, however, that the decision refers to the government's, not the individual's, need for privacy.[148]

> Records when there are reasonable grounds to believe disclosure may result in a safety risk, including the risk of harm to any person, any government-owned or leased institution or facility. . . . Such reasonable grounds shall be determined . . . with respect to records concerning any executive branch agency or the state or any municipal, district, or regional agency, by the Commissioner of Public Works, after consultation with the chief executive officer of the agency.

Id. This provision was applied in an ambiguous manner by the Connecticut Supreme Court in *Director, Department of Information Technology v. Freedom of Information Commission*, 874 A.2d 785 (Conn. 2005). *See supra* notes 91-92 and accompanying text.

[143] CONN. GEN. STAT. § 1-211(a) (2005).

[144] CONN. GEN. STAT. § 1-205 (2005).

[145] Superintendent of Police v. Freedom of Info. Comm'n, 609 A.2d 998, 1000 (Conn. 1992) (internal quotations omitted) (holding that, in keeping with policy of FOIA favoring disclosure and requiring that exceptions to disclosure be narrowly construed, city police department did not satisfy burden of "proving municipal permits to carry pistols were 'similar' to exempt medical and personnel files").

[146] Dir., Dep't of Info. Tech. v. Freedom of Info. Comm'n, 874 A.2d 785, 791 (Conn. 2005). *See supra* note 80 and accompanying text.

[147] Wilson v. Freedom of Info. Comm'n, 435 A.2d 353, 357 (Conn. 1980) (holding that state university program review committee documents were predecisional and university's reasons for refusing disclosure were sufficient to justify withholding documents).

[148] *Id.*

[48] Neither the Connecticut Legislature nor the Freedom of Information Commission appears to have recognized the consequences of the technological inversion that has occurred as a consequence of digital technologies and the Internet. The Connecticut Supreme Court in its decision in *Director, Department of Information Technology v. Freedom of Information Commission,* also demonstrated a profound lack of understanding of the consequences of the new technologies.[149]

C. SALE OF INFORMATION

[49] Even more disconcerting, perhaps, than the approach to administering the FOILs and the posting of information on websites is the sale of government databases. Some state and local governments have sought to reap economic benefit from their databases by selling them commercially.[150] Often, these sales take place without public knowledge, sometimes creating a backlash. One example is the sale of state motor vehicle records by some states.[151] In 1989, Rebecca Shaeffer, an actress, was murdered by a "fan" who learned her home address from a private investigator who had obtained it from California motor vehicle records. [152] Ms. Schaeffer's murder spurred Congress to enact the Driver's Privacy Protection Act.[153] The Act prohibits, with some exceptions, state motor vehicle departments from making available to any person or entity personal information about any individual.[154] The Act survived a

[149] Dir., Dept. of Info. Tech., 874 A.2d 785. *See supra* notes 80-93 and accompanying text.
[150] BARRETT & GREENE, *supra* note 20, at 173.
[151] *See* Travis v. Reno, 163 F.3d 1000, 1002 (7th Cir. 1998) (noting that the Wisconsin Department of Transportation makes approximately eight million dollars each year from the sale of motor vehicle information); Dan Christensen, *Driven to Sue: Suits in West Palm Beach Allege Personal Information On State's 13 Million Drivers Being Sold Unlawfully*, BROWARD DAILY BUSINESS REVIEW, June 24, 2003, at 1 (explaining that state of Florida did not sell data but named in suit).
[152] Margan v. Niles, 250 F. Supp. 2d 63, 68 (N.D. N.Y. 2003) (citing 139 Cong. Rec. S15745-01, S15765, S15762, S15761-66 (1993); 145 Cong. Rec. S14533-02, S14538 (1999)); *see infra* note 163; *see also* John Caher, *Municipalities May Be Liable Under Privacy Law for Drivers*, N.Y. L.J., March 20, 2003, at 1.
[153] Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (2000); *Margan*, 250 F. Supp. 2d at 68-69.
[154] 18 U.S.C. § 2721(a)(1).

constitutional challenge by South Carolina in the United States Supreme Court.[155]

[50] Notwithstanding the Act and the United States Supreme Court decision, the Connecticut Supreme Court has continued to support FOIL requests for motor vehicle data by giving a crabbed, narrow construction to the Driver's Privacy Protection Act. For purposes of implementing a personal property tax on automobiles, Connecticut statutes require that the Motor Vehicle Commissioner furnish town tax assessors with a list of names and addresses of owners of motor vehicles "using the records of the Department of Motor Vehicles."[156] For example, in *Davis v. Freedom of Information Commission*, an insurance investigator sought to examine the motor vehicle grand list books of the City of Bridgeport, and the tax assessor's office denied the request. [157] The Connecticut Freedom of Information Commission ordered the City to provide access to the motor vehicle grand list books.[158] The tax assessor challenged the Commission's decision.[159] The Commission's decision was upheld by both the Superior Court[160] and the Supreme Court of Connecticut, which adopted the opinion of the Superior Court. [161] The Superior Court reasoned that, although the Driver's Privacy Protection Act "regulates the disclosure of personal information contained in the records of motor vehicle departments,"[162] by *permitting* disclosure of the information to other governmental agencies for use in carrying out their functions, those records, when transferred, lost their protected status.[163]

[155] Reno v. Condon, 528 U.S. 141 (2000).
[156] CONN. GEN. STAT. § 14-163 (1999 & Supp. 2005).
[157] Davis v. Freedom of Info. Comm'n, 790 A.2d 1188, 1190 (Conn. Super. Ct. 2001).
[158] *Id.*
[159] *Id.*
[160] *Id.* at 1194.
[161] Davis v. Freedom of Info. Comm'n, 787 A.2d 530, 536-37 (Conn. 2002).
[162] *Davis*, 790 A.2d at 1192 (quoting Reno v. Condon, 528 U.S. 141, 143 (2000)).
[163] *Davis*, 790 A.2d at 1192-93 (emphasis added). A contrary view of the scope and reach of the Driver's Privacy Protection Act was expressed by a U.S. District Judge in New York who ruled that a town could be held vicariously liable for violation of the Driver's Privacy Protection Act because one of its police officers improperly "ran" license plate numbers and obtained information about plaintiffs from the New York Statewide Police Information Network. Margan v. Niles, 250 F. Supp. 2d 63, 66, 72-75 (N.D. N.Y. 2003).

[51] Through their somewhat tortured and circular reasoning,[164] the Connecticut courts gave greater weight to the literal provisions of the Connecticut FOIA than to the federal statute that had been upheld by the U.S. Supreme Court in the face of constitutional challenge,[165] thus ignoring the Supremacy Clause of the U.S. Constitution.[166] It has been clear, of course, at least since *Ableman v. Booth*,[167] that state courts cannot condone a violation of federal law.[168] In *Davis*, the Connecticut Supreme Court, in an effort to avoid weakening the Connecticut FOIA, effectively undermined Congress' attempt to protect the privacy of residents' motor vehicle information.[169] Yet, as in the town of Greenwich GIS case,[170] it is difficult to understand how *Davis*[171] advances the underlying purposes of a FOIL. Both decisions ignore the information privacy interests of residents.

IV. SOLUTIONS

[52] Solutions available to protect information privacy include legislative amendments to FOILs and aggressive assertion of federal statutory and Constitutional remedies by residents and local governments. As a policy matter, it would be far preferable for state legislatures to address these issues rather than to place the burden upon individual local governments and individual residents.

A. STATE LEGISLATURES

[53] Although some piecemeal bills have been introduced in state legislatures to address aspects of the impact of FOILs upon information

[164] The Department of Motor Vehicles was required by State law to transfer the information. CONN. GEN. STAT. § 14-163 (2004).
[165] *See Condon*, 528 U.S. at 148-51 (holding that the Driver's Privacy Protection Act of 1994 did not violate federalism principles and was a proper exercise of commerce power by Congress).
[166] *See* U.S. CONST. art. VI, cl. 2.
[167] 62 U.S. (21 How.) 506 (1858).
[168] *See id.* at 525-26 (rejecting the authority of the Wisconsin Supreme Court to refuse to adhere to the Federal Fugitive Slave Act).
[169] *Davis*, 787 A.2d at 536-37 (affirming and incorporating the Connecticut Superior Court decision); *see Davis*, 790 A.2d 1188.
[170] *Dir., Dept. of Info. Tech.*, 874 A.2d at 785.
[171] *Davis*, 790 A.2d 1188.

privacy,[172] there is little evidence of any desire to address these issues in a comprehensive manner.

[54] State legislative proposals for restrictions upon availability of information are fought ardently by "good government" organizations and FOIL advocates. Characterizing the reaction as "ideological drift," Professor Daniel Solove, citing Professor Jack M. Balkin, writes:
Ideological drift in law means that legal ideas and symbols will change their political valence as they are used over and over again in new contexts. Laws fostering transparency are justified as shedding light into the dark labyrinths of government bureaucracy to expose its inner workings to public scrutiny…. However, sunshine laws are increasingly becoming a tool for powerful corporations to collect information about individuals to further their own commercial interests, not to shed light on the government. A window to look in on the government is transforming into a window for the government and allied private sector entities to peer in on individuals.[173]
Whether state legislatures come to recognize the ideological drift will be crucial to the information privacy of residents.

B. RESIDENTS

[55] What legal options are available to residents who wish to avoid having personally identifiable information about them disseminated in electronic format by agencies in response to FOIL requests? In order to trump state FOIL laws, either federal statutes or Constitutional remedies

[172] *See, e.g.*, An Act Concerning the Disclosure of Geographic Information System Data, H.B. 5014, 2003 Gen. Assem., Jan. Sess. (Conn. 2003) (proposing to exempt from Connecticut FOIA disclosure all GIS data that concerns private residences and buildings); s*ee also* CONN. GEN. STAT. § 1-217(a) (2000 & Supp. 2005) (providing for nondisclosure of residential addresses of judges, police officers, and certain other specified officials and enacted in 1995); *see also*, Tobin A. Coleman, *Changes proposed for Sunshine Law*, Greenwich Time, Mar. 18, 2006, at A1 (reporting upon several proposed changes to the Connecticut FOIA under consideration in the State Legislature, with limited likelihood that any of the proposals will be enacted into law).
[173] Solove, *supra* note 14, at 1197 (internal citations omitted). *But* s*ee* Investigation Tech. v. Horn, 798 N.Y.S.2d 345, 345 (Sup. Ct. 2004) (denying Investigation Technologies' application compelling the New York City Department of Corrections to disclose birthdates of all detainees).

must be invoked.[174] First, in order to invoke any of the remedies available, the resident must know of the potential release of the information.[175] The arguments made in this section lead to the conclusion that residents may have to be notified about pending FOIL requests involving their personally identifiable information.[176]

1. STATUTORY REMEDIES

[56] The few available federal statutory remedies regulating records held by state and local governments address narrow strands of information.

---

[174] Neither the New York nor the Connecticut state constitution has been interpreted to provide protection for information privacy. *See, e.g.*, Pane v. City of Danbury, 841 A.2d 684, 691-94 (Conn. 2004) (finding neither Constitutional nor statutory claims for invasion of privacy based upon improper disclosure of information by city under Connecticut FOIA).

[175] Most often, residents do not know about a request for data that includes them. Some FOILs include provisions precluding the release of information about certain groups of people. *See, e.g.*, *supra* notes 141 and 163 and accompanying text. It is unlikely that an agency, when responding to a request for a large database, actually redacts specific information about certain groups of people in the database, particularly when the agency may not be aware, without canvassing the data subjects, that particular people fall within the protected group. *See* Liptak, *supra* note 44, at A12 (regarding the publication of information about Washington State police). In contrast, the OMB Memorandum regarding the conduct of Privacy Impact Assessments at least asks agencies to analyze and describe how people will have the opportunity to consent to particular uses of the information. *See* OMB Memorandum, *supra* note 105, at 2188. This is perhaps belated recognition of the recommendation made by the Department of Health, Education & Welfare in 1973:

> [W]e recommend that the Freedom of Information Act be amended to require an agency to obtain the consent of an individual before disclosing in personally identifiable form exempted-category data about him, unless the disclosure is within the purposes of the system as specifically required by statute. Pending such amendment of the Act, we further recommend that all Federal agencies provide for obtaining the consent of individuals before disclosing exempted-category personal data about them under the Freedom of Information Act.

U.S. DEP'T OF HEALTH, EDUC. & WELFARE, *supra* note 23 at 65-66, *available at* http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm (follow "IV. Recommended Safeguards for Administrative Personal Data Systems" hyperlink).

[176] If a large database is the subject of the request, the notification could be by publication or other mechanism for providing general notice to the public. *See, e.g.*, CALIF. CIV. CODE § 1798.29(g) (West Supp. 2005) (listing a variety of mechanisms to provide notice to those affected by state agency breaches of information security).

These statutes include the Driver's Privacy Protection Act,[177] the Family Educational Rights and Privacy Act,[178] and Section 7 of the Privacy Act.[179]

[57] Section 7(a) of the Privacy Act provides substantial privacy protection for residents' social security numbers by making it "unlawful for any Federal, State, or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number."[180]

[58] In addition, requests for a resident's social security number must include the following notice:

> Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.[181]

A court of appeals decision determined that Section 7 confers a private right enforceable under 42 U.S.C. §1983,[182] thus providing potent

[177] *See supra* notes 153-55 and accompanying text.
[178] Family Educational Rights & Privacy Act (FERPA), 20 U.S.C.A. § 1232(g) (1990 & Supp. 1991) (addressing student records in schools and colleges). For a thorough discussion of laws and regulations affecting privacy of student information, see NATIONAL FORUM ON EDUCATION STATISTICS, FORUM GUIDE TO PROTECTING THE PRIVACY OF STUDENT INFORMATION: STATE AND LOCAL EDUCATION AGENCIES (2004).
[179] Privacy Act of 1974, Pub. L. No. 93-579, § 7, 88 Stat. 1896, 1909 (1974).
[180] § 7(a)(1), 88 Stat. at 1909.
[181] § 7(b), 88 Stat. at 1909.
[182] Schwier v. Cox, 340 F.3d 1284 (11th Cir. 2003) (challenging Georgia voter registration procedures requiring voters to disclose social security numbers).

protection, with some exceptions,[183] from disclosure of a resident's social security number sought for burgeoning e-government databases.[184]

2. CONSTITUTIONAL REMEDIES

[59] The most effective legal instrument for preventing disclosure of most personally identifiable information is the United States Constitution. The privacy spotlight should be on the prevention of *disclosure*, particularly the disclosure in digital format, of information in state and local government databases rather than upon preventing the *collection* of that information. From a practical standpoint, it will be next to impossible to halt the expansion of e-government and the concomitant collection of information about residents in databases.[185] Consequently, the constitutional focus should address curtailing the copying and dissemination requirements of FOILs, particularly the copying in electronic, digital format.

---

[183] Section 7 of the Privacy Act does not apply to a disclosure required by federal statute or disclosure for a system of records in operation before January 1, 1975, which then required a social security number to identify an individual. § 7(a)(2)(B), 88 Stat. at 1909. In addition, the Tax Reform Act of 1976 authorized states to use social security numbers only "in the administration of any tax, general public assistance, driver's license, or motor vehicle registration." 42 U.S.C. § 405(c)(2)(C)(i) (2003).

[184] The Supreme Court has ruled that 5 U.S.C. § 552a(g)(4)(A), which makes the federal government liable under Section 3 of the Privacy Act for actual damages, requires proof of some actual damages to recover the $1,000 minimum statutory damages. Doe v. Chao, 540 U.S. 614 (2004).

In addition, remedies may exist under state law. In an interesting decision, the New Hampshire Supreme Court, in response to a certified question from the United States District Court for the District of New Hampshire, held that:

> [W]hile a SSN [social security number] must be disclosed in certain circumstances, a person may reasonably expect that the number will remain private . . . . Accordingly, a person whose SSN is obtained by an investigator from a credit reporting agency without the person's knowledge or permission may have a cause of action for intrusion upon seclusion for damages caused by the sale of the SSN, but must prove that the intrusion was such that it would have been offensive to a person of ordinary sensibilities.

Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1008-1009 (N.H. 2003). The sale of the social security number and later her workplace address by an internet-based investigation service had led to the killing of the plaintiff's twenty-year-old daughter at her workplace. *See, e.g.*, John Riley, *Legal Heat for Detective Ruse: Technique Helped a Stalker to Kill*, NEWSDAY, March 16, 2003, at A8; O'HARROW, *supra* note 5, at 148-149.

[185] *See supra* Part II.A.

[60] The source of the constitutional right to information privacy derives from a combination of the Fourth Amendment and the liberty interest of the Fifth and Fourteenth Amendments.[186] The delineation of constitutional rights involved is now at a nascent stage similar to that which faced the United States Supreme Court in 1928 when it considered the Fourth Amendment privacy issues created by the telephone in the case of *Olmstead v. United States.*[187] The place of the telephone in United States society was evolving rapidly in the late 1920s, and Fourth Amendment doctrine was facing challenges from both technological inversion and ideological drift. Although the Court's five-to-four decision held that an off-premises wiretap was not a search, [188] the majority opinion failed to appreciate the impact of the telephone. Justice Brandeis, writing for the dissent, wrote with a Jeffersonian sense of future developments:

> But time works changes, brings into existence new conditions and purposes. Subtler and more far-reaching means of invading privacy have become available to the government . . . . Moreover, in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be.[189]

[61] It took another thirty-nine years for a majority of the Court to recognize the changes wrought by the telephone. In *Katz v. United States*,[190] the Court held that a bug placed on top of a glass public telephone booth was a search because the bug constituted the "uninvited ear" from which United States citizens are protected by the Fourth Amendment.[191] In today's world, the combination of technological inversion and the rapid advances in digitalizing public administration create a similar situation to that of *Katz*, in which FOIL laws are leading to an invasion of the Americans' constitutional right to privacy in their personal information.

---

[186] U.S. CONST. amend. IV, V, XIV.
[187] Olmstead v. United States, 277 U.S. 438 (1928).
[188] *Id.* at 464.
[189] *Id.* at 473-74 (Brandeis, J., dissenting) (internal quotations omitted).
[190] 389 U.S. 347 (1967).
[191] *Id.* at 352.

[62] The Supreme Court has recognized a constitutional right to privacy in personal information, which has been applied in different contexts by several United States Courts of Appeals. "One element of privacy has been characterized as 'the individual interest in avoiding disclosure of personal matters.'"[192] Personal information is recognized as included within the concept of personal matters. In *Whalen v. Roe*,[193] the Court upheld the constitutionality of a New York law that required physicians to report certain drug prescriptions to the state in part because of privacy protections included within the statutory scheme. The Supreme Court stated:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory *duty to avoid unwarranted disclosures*. Recognizing that in some circumstances that duty arguably *has its roots in the Constitution*, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy.[194]

[63] The Supreme Court has also explicitly recognized the distinction between individual public records, which are subject to public view but

[192] Nixon v. Adm'r of Gen. Serv., 433 U.S. 425, 457 (1977) (quoting Whalen v. Roe, 429 U.S. 589, 599 (1977)) (rejecting claim of presidential privilege and upholding Presidential Recordings and Materials Preservation Act of 1974 after weighing former President Nixon's privacy interest in avoiding disclosure of personal matters against governmental interest expressed in the Act).
[193] 429 U.S. 589 (1977).
[194] *Id.* at 605 (emphasis added).

protected by practical obscurity,[195] and public records in a compilation. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*,[196] the Court denied a Federal FOIA request for an FBI "rap sheet," a compilation of scattered criminal records, by invoking a somewhat labored interpretation of the Federal FOIA to avoid the need to address the constitutional issues potentially involved in the case.[197] The Court in *Reporters Committee* restated one of the *Whalen* principles as follows: "[O]ur cases have also recognized the privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public."[198] The Court then elaborated: "[w]e have also recognized the privacy interest in keeping personal facts away from the public eye."[199]

[64] One commentator has analyzed which types of information implicate informational privacy interests:

> The extent to which specific types of information implicate privacy often may be a by-product of two interrelated factors: the intrinsic and consequential features of the information. Intrinsic features involve the degree of intimacy of the information. Consequential features involve the potential for harm to the subject if the information is disclosed. Information may not be intimate and yet may be considered "highly personal" by a reasonable person because of the fear that the disclosure would bring harmful or embarrassing consequences.[200]

Another commentator has discussed the consequences of not recognizing the privacy implications of "personal" information:

> The creeping loss of privacy that arises from narrowly defining personal information and exempting public information from protection calls for a reevaluation of U.S.

[195] *See supra* notes 23-24 and accompanying text.
[196] 489 U.S. 749 (1989).
[197] *Id.* at 762, n.13.
[198] *Id.* at 767; *see also* comment of Mr. Davis, *supra* note 108 and accompanying text.
[199] *Id.* at 769.
[200] Richard C. Turkington & Anita L. Allen, PRIVACY LAW: CASES AND MATERIALS 384 (1999).

> policy toward public information. The need for personal information to be "public information" must be identified clearly and narrowly. This reduces the erosion of public and private distinctions and the corresponding loss of citizen privacy. At the same time, the use of public information should be restricted to the purpose for which the personal information was made public. Such a policy promotes basic fairness in the treatment of personal information and minimizes the adverse impact on privacy without compromising the objectives of open government.[201]

[65] The FOILs' requirements for disclosing and copying of government-held information embody values of transparency in government decision making and integrity in government administration. These interests should be weighed against constitutional rights involving personal liberties, including the constitutional right to privacy of personal information (information privacy), which was built upon "the right to be let alone."[202] In defining the Fourth Amendment right to privacy, the Supreme Court in *Katz v. United States*[203] asked whether a person has a legitimate expectation of privacy in an invaded place.[204] The Court elaborated in a later case by explaining that the scope of the Fourth Amendment protection extends where the citizen has manifested a subjective expectation of privacy, and that expectation is one that society accepts as objectively reasonable.[205]

---

[201] Joel R. Reidenberg, *International Approaches to Public and Private Sector Data Privacy and Security, in* A LITTLE KNOWLEDGEE: PRIVACY, SECURITY, AND PUBLIC INFORMATION AFTER SEPTEMBER 11 100 (Peter M. Shane, John Podesta, & Richard C. Leone eds., 2004). The Chief of the Office of Privacy Protection of the California Department of Consumer Affairs, commenting about the increasing concerns about identity theft, stated: "The role played by public records containing Social Security numbers and other sensitive personal information is critical. It's time to reconsider how we can keep an eye on government without spying on individual citizens and without exposing them to the risk of identity theft." Yuill, *supra* note 19, at 2430. *See infra* note 208 and accompanying text regarding the prevalence of identity theft.

[202] *See infra* notes 212-213 and accompanying text.

[203] 389 U.S. 347 (1967).

[204] *Id.* at 353.

[205] California v. Greenwood, 486 U.S. 35, 39 (1988) (holding that a warrantless search of garbage bags left at curb violates Fourth Amendment only if there is subjective

[66] The increasing reliance upon and importance of personally identifiable information in essence creates and defines a "virtual person," described by one commentator as a "digital persona" that approximates personality. [206] "[T]he digital persona is a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual."[207] A person cannot function normally in today's United States without a social security number, driver's license, bank accounts, credit and debit cards, etc. It is also virtually impossible for a person to function if his or her personally identifiable information is widely disseminated to others, creating the opportunity for identity theft, which is perhaps the fastest growing crime in the United States.[208] Business and commerce have recognized the value of information about people in many contexts, and corporations go to great lengths to acquire such information, often, as already noted, from public agency databases.[209] The United States Supreme Court has acknowledged that personally identifiable information is a valuable article of commerce.[210]

[67] Consequently, individual constitutional privacy rights should now encompass the virtual person or digital persona. A United States Court of Appeals decision stated that the Supreme Court has recognized a right to

expectation of privacy that society finds objectively reasonable, but finding no violation in these circumstances) .

[206] Roger Clarke, *The Digital Persona and Its Application to Data Surveillance,* THE INFORMATION SOCIETY, 10(2), *2 (1994), *available at* http://www.anu.edu/people/Roger.Clarke/DV/DigPersona.html.

[207] *Id.*

[208] *See, e.g.*, Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem,* 80 TEX. L. REV. 89 (2001) (discussing scope of and consequences to victims of identity theft). The Federal Trade Commission collects statistics regarding the incidence of identity theft. Federal Trade Commission: Your National Resource About ID Theft, *available at* http://www.consumer.gov/idtheft/id_federal.htm (last visited Oct. 24, 2005); *see also* Senator Maria Cantwell: Fighting Identity Theft, http://cantwell.senate.gov/issues/ID/statistics.cfm (last visited Jan. 23, 2006) (identity theft statistics collected from several sources by U.S. Senator Maria Cantwell); Yuill, *supra* note 19.

[209] *See supra* notes 14-15 and accompanying text; *see also, e.g.,* Paul M. Schwartz, *Property, Privacy, and Personal Data,* 117 HARV. L. REV. 2055 (2004) (proposing a model of propertized personal information that would respond to privacy concerns).

[210] Reno v. Condon, 528 U.S. 141 (2000).

confidentiality, [211] a subset of "the right to be let alone," originally observed by Justice Brandeis in his *Olmstead* dissent:

> They [the makers of our Constitution] conferred, as against the Government, the right to be let alone–the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[212]

Given the increasing importance of the new virtual person, the *Katz* test[213] should be applicable to the government's control and dissemination of personally identifiable information. Although the government may extract information from a resident for a valid purpose, a *Katz* expectation of privacy may nonetheless exist with respect to the information unwillingly surrendered to the government. The propriety of the government seizing personal information is based in part upon the government's purpose and the use made of the information. A valid intrusion by the government, however, may become unjustifiable when it escapes its original purpose. When the government publishes validly obtained information, it nevertheless may intrude upon a subjective expectation of privacy on the part of the resident that society would accept as reasonable. It violates the *Katz* test by misusing the information, thus breaching the right to informational privacy.[214]

[68] The potential consequences of the availability from government entities of personally identifiable information also affect the liberty

[211] Doe v. City of New York, 15 F.3d 264 (2d Cir. 1994).
[212] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).
[213] Katz v. United States, 389 U.S. 347 (1967).
[214] The circumstances are analogous to other situations in which the government validly collects information for one purpose and then seeks to use it for other purposes. *See, e.g.*, D.H. Kaye, *The Constitutionality of DNA Sampling on Arrest*, 10 CORNELL J.L. & PUB. POL'Y 455 (2001) (examining the constitutionality of taking, analyzing, storing, and using DNA samples and data from arrested persons). The author's discussion of "special needs" searches is particularly relevant. *Id.* at 489-98. *See also*, Monica R. Shah, Note, *The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace*, 105 COLUM. L. REV. 250 (2005) (questioning the admissibility of criminal evidence acquired by private-citizen hackers and turned over to the police).

interest of preserving the privacy of personal information. Building upon the Supreme Court decisions in *Meyer v. Nebraska,*[215] *Ingraham v. Wright,*[216] *Cruzan v. Missouri Dep't of Health,*[217] and *Planned Parenthood of Southeastern Pennsylvania v. Casey,*[218] the Sixth Circuit found that:

> Individuals have a clearly established right under the substantive component of the Due Process Clause to personal security and to bodily integrity, and this right is fundamental where the magnitude of the liberty deprivation that the abuse inflicts upon the victim . . . strips the very essence of personhood.[219]

As a consequence, the Sixth Circuit "found that the [City of Columbus undercover police] officers have a fundamental constitutional interest in preventing the release of personal information contained in their personnel files where such disclosure creates a substantial risk of serious bodily harm,"[220] and, consequently, that the City must demonstrate that its "actions narrowly serve a compelling public purpose."[221]

---

[215] Meyer v. Nebraska, 262 U.S. 390, 399 (1923) (noting that there are "privileges long recognized at common law as essential to the orderly pursuit of happiness by free men").
[216] Ingraham v. Wright, 430 U.S. 651, 673 (1977) (recognizing the "right to be free from … unjustified intrusions on personal security").
[217] Cruzan v. Missouri Dep't of Health, 497 U.S. 261, 278 (1990) ("acknowledging that a competent person has a constitutionally protected liberty interest under the Fourteenth Amendment in refusing unwanted medical treatment" (quoting Kallstrom v. City of Columbus, 136 F.3d 1055, 1062 (6th Cir. 1998))).
[218] Planned Parenthood of Southeastern Pennsylvania v. Casey, 505 U.S. 833, 857 (1992) ("stating that the right to an abortion reflects respect for 'personal autonomy and bodily integrity'" (quoting *Kallstrom*, 136 F.3d at 1062)).
[219] *Kallstrom*, 136 F.3d at 1062-63 (internal quotations omitted).
[220] *Id.* at 1064. The personal information included, among other information, the officers' addresses, telephone numbers, copies of their drivers' licenses, and immediate family members' names, addresses and telephone numbers. *Id.* at 1059.
[221] *Id.*; *cf.* Liptak, *supra* note 44 (describing the experience of Washington State police officers). The threat to personal security often applies to people outside of the law enforcement field and may be quite unpredictable. *See* text accompanying *supra* note 152 (discussing the murder of actress Rebecca Shaeffer); *supra* note 166 (discussing the workplace murder of Ms. Remsburg's daughter). *See also supra* note 142 and accompanying text (identifying the exemption in the Connecticut FOIA for residential addresses of public officials, including judges and police officers, a legislative recognition that the release of addresses places these officials in jeopardy).

[69] Another important element of the *Kallstrom* case is the issue of notice to those affected by the release of information. Although the Ohio Public Records Act[222] did not require notice to affected people prior to the release of information, the Sixth Circuit found a constitutional requirement for prior notice in this case under the procedural due process component of the Fourteenth Amendment:

> The procedural component of the Fourteenth Amendment's Due Process Clause, however, at a minimum requires that the City notify the officers of a request for their addresses, phone numbers, and driver's licenses, and the names, addresses, and phone numbers of their family, prior to releasing this information so that they may have the opportunity to invoke their constitutionally protected rights to privacy and personal security.[223]

The right to privacy in personal information is affected crucially by the purposes for and methods by which governments obtain personally identifiable information from their residents. Several purposes for governmental collection of information can be differentiated: supporting the exercise of a fundamental constitutional right (i.e., voting and jury service), fulfilling obligations created by the government (i.e., paying taxes, compulsory school attendance, and filing land records), satisfying requirements essential to one's livelihood (i.e., professional and business licenses, drivers' licenses), and seeking access to services provided by the government (i.e., libraries, parks, public universities, and public hospitals). The virtual person's right to be let alone is particularly compelling when the government has forced disgorgement of the personally identifiable information into an electronic database (as is the case in most programs today) and then seeks to distribute it broadly, most often without notice to the affected residents.[224] "[W]hen the information is in the Government's control as a compilation, rather than a record of '*what the Government is up to*,' the privacy interest . . . is in fact at its apex, while the FOIA-based

[222] OHIO REV. CODE ANN. § 149.43 (West 1997).
[223] *Kallstrom*, 136 F.3d at 1067.
[224] *See* Greidinger v. Davis, 988 F.2d 1344, 1345 (4th Cir. 1993); *see also infra* notes 229-31 and accompanying text.

public interest in disclosure is at its nadir."[225] Both the *Whalen* and *Reporters Committee* decisions emphasize, in the words of *Whalen,* that "[t]he right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory *duty to avoid unwarranted disclosures*. . . . [I]n some circumstances that duty arguably *has its roots in the Constitution* . . . ."[226] The standard of review or degree of scrutiny applicable to the government's actions and the weight given to the government's interests, as well as the reasonableness of an expectation of privacy, vary depending upon the governmental purpose involved in the data collection and maintenance.

A. STRICT SCRUTINY AND FUNDAMENTAL RIGHTS

[70] "Where certain 'fundamental rights' are involved, the Court has held that regulation limiting these rights may be justified only by a 'compelling state interest,' and that legislative enactments must be narrowly drawn to express only the legitimate state interests at stake."[227] In other words, strict scrutiny must be applied. If the disclosure of personal information is required as a condition of the exercise of a fundamental right, such as the right to vote or the right to serve on a jury, then strict scrutiny should be applied to the state's desire to disclose and make this information available in electronic format to the public.[228] Similarly, if the failure to provide information required to fulfill obligations mandated by the government, such as paying taxes and attending school, will result in sanctions such as the deprivation of liberty, then strict scrutiny should also be applied to the state's desire to disclose and make this information available in electronic format to the public.

---

[225] United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 780 (1989) (emphasis added) (referring to Federal FOIA exemption 7(c), but applicable as well to the constitutional issue).

[226] Whalen v. Roe, 429 U.S. 589, 605 (1977) (emphases added); *see Reporters Comm.*, 489 U.S. 749.

[227] Roe v. Wade, 410 U.S. 113, 155 (1973) (citations omitted).

[228] The "fundamental right of access to the courts," *Tennessee v. Lane*, 541 U.S. 509, 533-34 (2004), and the concomitant impact of the availability of court filings in electronic format on the Internet are beyond the scope of this article. The latter is, however, a topic of lively debate. *See supra* note 105.

[71] In *Greidinger v. Davis*,[229] the Fourth Circuit ruled that conditioning the right to vote upon a citizen making available his or her social security number, which then became subject to public disclosure, "compel[led] a would-be voter in Virginia to consent to the possibility of a profound invasion of privacy when exercising the fundamental right to vote."[230] The Fourth Circuit concluded that "it creates an intolerable burden on that right as protected by the First and Fourteenth Amendments."[231]

[72] Strict scrutiny has also been found applicable when the release of personal information contained in personnel files creates a "substantial risk of serious bodily harm,"[232] As already noted, the threat of substantial risk of bodily harm may apply to people not in the law enforcement enterprise.[233] Consequently, the release of other records, such as motor vehicle records and even GIS records may in some cases trigger a substantial risk of bodily harm.[234]

B. INTERMEDIATE SCRUTINY

[73] If, however, the disclosure of information is a consequence of information received by the government by a resident seeking to obtain important but not indisputably essential services, such as a driver's license, automobile registration, or the filing of property records, then intermediate scrutiny may be the appropriate standard for evaluating challenges to the government's disclosure requirements. The intermediate scrutiny standard of review as usually formulated requires the government to establish that its requirements "serve important governmental objectives and must be substantially related to achievement of those objectives."[235] It has been applied most often, but not exclusively, in cases involving gender discrimination.[236]

---

[229] Greidinger v. Davis, 988 F.2d 1344 (1993).
[230] *Id.* at 1354.
[231] *Id.* at 1355. *See also* Schwier v. Cox, 340 F.3d 1284, 1291-92 (11th Cir. 2003).
[232] Kallstrom v. City of Columbus, 136 F.3d 1055, 1064 (6th Cir. 1998). *See supra* notes 219-23 and accompanying text.
[233] *See supra* note 221.
[234] *See supra* text accompanying notes 151-152.
[235] Craig v. Boren, 429 U.S. 190, 197 (1976) (finding that Oklahoma gender-based distinction involving sale of 3.2% beer was denial of equal protection).
[236] *See, e.g.*, Nev. Dep't of Human Res. v. Hibbs, 538 U.S. 721 (2003) (upholding constitutionality of Family Medical Leave Act of 1993 as applied to the states); United

[74] If the Court applies intermediate scrutiny to such a challenge by a resident, then the government must come forward with a substantial interest in disclosing this information in digital compilations that outweighs individual privacy interests. In the light of the *Whalen* and *Nixon* decisions,[237] the Second Circuit concluded:

> [S]ome form of intermediate scrutiny or balancing approach is appropriate as a standard of review . . . . [A]n intermediate standard of review seems in keeping both with the Supreme Court's reluctance to recognize new fundamental interests requiring a high degree of scrutiny for alleged infringements, and the Court's recognition that some form of scrutiny beyond rational relation is necessary to safeguard the confidentiality interest.[238]

Applying intermediate scrutiny, the panel found a substantial state interest in the financial disclosure law enacted by the City of New York.[239] Although the statute permitted public inspection of the filings and "the degree of intrusion stemming from public exposure of the details of a person's life is exponentially greater than disclosure to government officials,"[240] the court stated that the statute's privacy mechanism "adequately protects plaintiffs' constitutional privacy interests."[241]

States v. Morrison, 529 U.S. 598 (2000) (holding federal civil remedy created by Violence Against Women Act of 1994 for victims of gender-motivated violence unconstitutional).

[237] Whalen v. Roe, 429 U.S. 589 (1977); Nixon v. Adm'r of Gen. Serv., 433 U.S. 425 (1977).

[238] Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir. 1983) (internal citations omitted) (evaluating public access to financial disclosure forms required to be filed by a substantial number of public employees of New York City).

[239] *Id.* at 1556, 1560; *see* NEW YORK CITY ADMIN. CODE § 1106-5.0 (1979) (requiring annual financial reports from many City officials but allowing any official to request that his report not be made available for public inspection because such inspection would constitute unwarranted invasion of privacy).

[240] *Barry*, 712 F.2d at 1561 (quoting Slevin v. City of New York, 551 F. Supp. 917, 934 (S.D.N.Y. 1982)).

[241] *Barry*, 712 F.2d at 1561. The statute permitted a covered employee to request redaction from disclosure of information filed in the disclosure forms although, at the time of the *Barry* decision, the efficacy of this privacy protection provision was untested. The information was also protected by practical obscurity inasmuch as the financial

[75] The collection of personally identifiable information by government for the purpose of operating a driver licensing system or a land records system undoubtedly serves important governmental objectives and is substantially related to the achievement of these objectives, but is the release of this information to the public, particularly in digital format, substantially related to the achievement of these objectives? The answer should be no with regard to the objectives of the licensing and recording system. The question becomes whether it is substantially related to the achievement of the objectives of the FOILs. When government's purpose is to serve its own administrative needs, not to assist in governmental decision making, then the answer should also be no. The release of compilations of personally identifiable information in digital format is not central to the purposes of FOILs. As the Supreme Court opined while considering the Federal FOIA in *Reporters Committee*, "the FOIA's central purpose is to ensure that the *Government's* activities be opened to the sharp eye of public scrutiny, not that information about *private citizens* that happens to be in the warehouse of the Government be so disclosed."[242] The information privacy principle that governs requests for information about a particular private citizen is equally if not more applicable to requests for information about many citizens. In addition, the information is almost always available through the components that fed the compilation or with redaction of the identifiers in releases in analog form.

C. UNCONSTITUTIONAL CONDITIONS

[76] In many circumstances, information is supplied to the government by residents seeking access to its services, such as parks and libraries. In these instances, the government is not forcing the disgorging of information, but requiring and collecting the information as a condition of making one of its services available. This article has examined computerized information systems in use by parks and recreation departments[243] and discussed library information systems.[244] Personally

disclosure form was available only in hard copy at an administrative office. NEW YORK CITY ADMIN. CODE § 1106-5.0 (1979).

[242] United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 774 (1989).

[243] *See supra* note 94 and accompanying text.

identifiable information is collected and retained in these state and local government databases in order to administer the programs efficiently. Under state FOILs, however, it is available to requesters in electronic form, without notice to the residents.

[77] In order to avail themselves of the public service, residents are required to provide personally identifiable information and, usually unknowingly, to permit unlimited access to that information, leaving them with no ability to exercise their constitutional right to information privacy. Consequently, they must submit to an unconstitutional condition that violates their right to information privacy if they want access to that public service. As long ago as 1926, the United States Supreme Court defined an unconstitutional condition:

> It would be a palpable incongruity to strike down an act of state legislation which, by words of express divestment, seeks to strip the citizen of rights guaranteed by the federal Constitution, but to uphold an act by which the same result is accomplished under the guise of a surrender of a right in exchange for a valuable privilege which the state threatens otherwise to withhold . . . . It is inconceivable that

[244] *See supra* note 96 regarding the increasing use of RFID tags in libraries. The increasing automation of library circulation systems has collided with the USA Patriot Act, § 215, 50 U.S.C. §§ 1861-63 (2001), engendering controversy regarding government access to information in library databases. On July 8, 2004, a proposed amendment in the House of Representatives to the Fiscal 2005 Justice Department appropriations bill (HR 4754, 111th Cong. (2004)) would have prohibited use of funds to acquire library circulation records or library patron lists. The amendment was rejected by a tie vote after voting was held open for 30 minutes by Republican leaders to convince members to change their votes. *Limits on Federal Search Powers*, CQ WKLY., Dec. 11, 2004, at 2923-2924. On June 15, 2005, however, the House approved, by a vote of 238-187, an amendment to the Fiscal 2006 Commerce-Justice-Science appropriations bill (HR 2862, 112th Cong. (2005)) that would prohibit the FBI from fully using § 215 of the USA Patriot Act. Seth Stern, *House Votes to Limit Patriot Act*, CQ WKLY., June 20, 2005, at 1649. The 2006 reauthorization of the USA PATRIOT Act (P.L. 109-178), by including a provision that libraries operating in traditional roles and not as internet service providers would not be subject to national security letters, should address some of the concerns. Michael Sandler, *Deal Clears Way for Anti-Terrorism Law*, CQ WKLY., Mar. 13, 2006, at 703.

> guaranties embedded in the Constitution of the United States may thus be manipulated out of existence.[245]

[78] The unconstitutional condition doctrine is now applied most often in the First Amendment context.[246] It should be equally applicable in the context of Fourth and Fourteenth Amendment privacy rights. Residents are asked to forsake their information privacy rights as a condition of availing themselves of state and local government services. The databases supporting these services are maintained for the convenience and efficiency of the government in administering the programs.[247] The information about individual residents is not used as a basis for governmental decisions and thus is not central to the purposes of FOILs. In addition, as previously discussed, there are options for making some or all of the information available in forms less threatening to information privacy rights of residents.[248] Similarly, the unconstitutional conditions doctrine is also applicable to the types of information disclosure considered in the preceding strict scrutiny and intermediate scrutiny sections.

C. STATE AND LOCAL GOVERNMENTS

[79] Local governments desiring to control the dissemination of their databases have several options. The haphazard manner in which decisions about collection, management, and release of personally identifiable information are now managed contributes significantly to the privacy problems they currently face.[249] Consequently, local governments should designate an official, either full time or part time, as the chief privacy

---

[245] Frost v. R.R. Comm'n, 271 U.S. 583, 593-4 (1926) (holding that California law requiring private automobile carriers for hire to obtain certificate and submit to regulation as common carrier exacted an unconstitutional condition and denied due process).

[246] *See, e.g.*, Legal Serv. Corp. v. Velazquez, 531 U.S. 533 (2001) (finding that a condition imposed by Congress (prohibiting representation involving effort to amend or challenge existing welfare law) on the use of Legal Services Corporation (LSC) funds violates the First Amendment rights of LSC grantees *and their clients*); Perry v. Sindermann, 408 U.S. 593, 597 (1972) (holding that government "may not deny a benefit to a person on a basis that infringes his constitutionally protected interests–especially, his interest in freedom of speech").

[247] Virtually all of these services were offered to residents in the era preceding the digital age.

[248] *See supra* Section IV.B.2.b.

[249] *See* WEST, *supra* note 98; *e.g.* Harmon, *supra* note 105 and accompanying text.

officer of the jurisdiction. As previously noted, few, if any, local governments currently have such a position.[250] The chief privacy officer should be given responsibility for overseeing and assessing the impact that decisions about collection and release of data and placement of data on the jurisdiction's internet website will have on individuals' privacy. The Office of Management and Budget Guidance on Implementing Privacy Provisions of the E-Government Act can serve as a model.[251] Focused, systematic, and coherent attention to privacy issues will raise the level of awareness within the governmental entity and among local residents and should reduce mistakes and inadvertent actions by public officials.

[80] Local governments do not have standing to raise privacy issues on behalf of residents.[252] Local officials can, however, notify affected local residents who then can litigate in their capacity as residents when a FOIL request presenting serious privacy concerns arises. Indeed, as a broader matter, local jurisdictions should undertake the practice of notifying residents about FOIL requests that involve their personally identifiable information. Notification can be made through notice in the local newspaper, a posting on the jurisdiction's website, e-mail to a list of residents who have requested notification, and by other means.[253] Under some circumstances, particularly when fundamental rights are affected, the jurisdiction may be constitutionally obligated to provide notice to those affected.[254]

[81] Another and potentially potent mechanism available to state and local jurisdictions is the judicious use of copyright. A copyright can provide a local jurisdiction with the legal ability to control redistribution

[250] *E.g.* BARRETTE & GREENE, *supra* note 20 and accompanying text.
[251] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899; s*ee supra* note 105.
[252] *See, e.g.*, Superintendent of Police v. Freedom of Info. Comm'n, 609 A.2d 998, 1002 (Conn. 1992) (holding that "[w]e have uniformly resisted the efforts of litigants to assert constitutional claims of others not in a direct adversarial posture before the court" (quoting Southern Connecticut Gas Co. v. Housing Authority, 468 A.2d 574 (1983)).
[253] The California Breach Law, effective July 1, 2003, provides for notifications regarding breaches of security by written notice, electronic notice, and substitute notice by e-mail when the agency has an e-mail address for the subject persons, conspicuous posting on the agency's website, and notification to major statewide media. CALIF. CIV. CODE § 1798.29(g) (2004).
[254] *E.g.* Kallstrom v. City of Columbus, 136 F.3d 1055, 1067 (6th Cir. 1998).

of information it provides in response to FOIL requests.[255] Use of copyright, however, raises a number of legal issues. Can the databases at issue be copyrighted? Does the state FOIL abrogate the authority of local governments to invoke copyright protection? Can the requirements of the FOIL be satisfied if copyright protection is invoked?

[82] All of these issues were addressed in an important Second Circuit case, *County of Suffolk, New York v. First American Real Estate Solutions,*[256] involving the attempt by Suffolk County to copyright and control redistribution of the County's official tax maps.[257] Having obtained the official tax maps from Suffolk County through a FOIL request, First American then marketed copies of the tax maps and CD-ROM disks containing the maps without the consent of or a license from the County.[258] The County initiated a legal action, alleging that its copyrights had been infringed.[259] Both the State of New York and the City of New York appeared as amici curiae before the Second Circuit.[260]

[83] Regarding the substantive issues, the Second Circuit panel first found, citing a number of precedents and authorities, that, under the Copyright Act, "states and their subdivisions are not excluded from protection under the Act."[261] Consequently, states and their subdivisions, unless prohibited from doing so by specific state law, may seek to copyright databases under their control.

---

[255] A fundamental right of the copyright owner is control of the distribution of the copyrighted material. 17 U.S.C. § 106(3) (2000).

[256] County of Suffolk, N.Y. v. First Am. Real Estate Solutions, 261 F.3d 179 (2d Cir. 2001).

[257] The tax maps and their index system provided the ownership, size, and location of real property in each of the County's political subdivisions. The maps are updated annually and cover over 500,000 parcels of land. *Id.* at 184.

[258] *Id.*

[259] *Id.* Once again, the typical pattern emerges. A corporation obtains a database from a governmental entity through a FOIL request and then markets the data. *See, e.g.* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement,* 29 N.C.J. INT'L L. & COM. REG. 595, 595-596 (2004).

[260] New York State and New York City also have sought to protect their GISs from uncontrolled distribution. Both filed amicus curiae briefs as the Second Circuit considered the case. *County of Suffolk,* 261 F.3d at 186.

[261] *Id.* at 187.

[84] The Second Circuit then addressed the issue of whether the tax maps were copyrightable. The panel concluded that, although "items such as street location and landmarks were 'physical facts'–and thus not protected elements– . . . the presentation of such physical facts could be original."[262] It further noted that even a slight amount of originality is sufficient for copyright and concluded that "Suffolk County has sufficiently alleged that its work is protected."[263] In reaching its conclusion, the panel relied to a significant degree upon the now classic Supreme Court decision in *Feist Publications, Inc. v. Rural Telephone Service Co.*[264] In reaching its conclusion that the white pages were not copyrightable, the Court distinguished between facts and compilations of facts:

> Copyright treats facts and factual compilations in a wholly consistent manner. Facts, whether alone or as part of a compilation, are not original and therefore may not be copyrighted. A factual compilation is eligible for copyright if it features an original selection or arrangement of facts, but the copyright is limited to the particular selection or arrangement. In no event may copyright extend to the facts themselves.[265]

[85] It is the creativity of the compilation that gives it the constitutionally required originality,[266] but the compilation need possess only "at least some minimal degree of creativity."[267] Because digital databases involve the use of a program or system, it is unlikely that any digital compilation would fail to meet the requirement of minimal creativity.

[86] The panel also concluded that the tax maps were not inherently in the public domain because of the need for an economic incentive to create the

---

[262] *Id.* at 188.
[263] *Id.*
[264] *Id.* 499 U.S. 340 (1991) (holding that telephone white pages book was not copyrightable because factual information lacked the requisite originality).
[265] *Feist*, 499 U.S. at 350-51.
[266] U.S. CONST., art. I, § 8, cl. 8 ("To promote the Progress of Science and Useful Arts, by securing for a limited time to Authors and Inventors the exclusive Right to their Respective Writings and Discoveries").
[267] *Feist*, 499 U.S. at 345.

work, and because they were not themselves necessary to give the public notice of the law.[268] Thus, the maps could be copyrighted.

[87] The panel then focused on the knotty question of whether the New York FOIL abrogated Suffolk County's copyright. After a careful analysis of the statute, rejecting a contrary interpretation by the State's Committee on Open Government, it concluded that there was no clear indication that the State Legislature intended to abrogate a covered entity's copyright:

> By the statute's plain language, the extent of the state agency's obligation is to make its records available for public inspection and copying. It is one thing to read this provision to permit a member of the public to copy a public record, but it is quite another to read into it the right of a private entity to distribute commercially what it would otherwise, under copyright law, be unable to distribute.[269]

[88] In what is perhaps the most important aspect of the opinion, the court concluded that Suffolk County could maintain its copyright protections while complying with its FOIL obligations.[270] The court reasoned that the New York FOIL does not explicitly address what a recipient can do once it receives agency records; it only requires that the agency make the records available for public inspection and copying.[271] "FOIL . . . does not prohibit a *state agency* from placing restrictions on how a record, if it were copyrighted, could be subsequently distributed."[272] The panel reasoned as follows:

> Suffolk County is not attempting to restrict *initial access* but is attempting to restrict only the *subsequent redistribution* of its copyrighted works. There is nothing inconsistent between fulfilling FOIL's goal of access and permitting a state agency to place reasonable restrictions on the redistribution of its copyrighted works. For example,

[268] *County of Suffolk*, 261 F.3d at 194-195.
[269] *Id.* at 189.
[270] *Id.* at 191.
[271] *Id*. at 192-93.
[272] *Id.* at 192.

> an agency's choice to notify the recipient that a portion of the record is protected by copyright law or an agency's requirement that the recipient enter into a licensing agreement if it wishes to distribute the record commercially does not restrict initial access but only what the recipient may do once it acquires access.[273]

[89] The Court cautioned that the County could not restrict subsequent dissemination completely because copyright protects only the form of expression and not the ideas expressed or the facts included and is subject to the fair use doctrine.[274] The form of expression, however, should incorporate the use of orthophotography and arc info coverages, as well as the SQL server databases referenced to GIS data.[275]

[90] The Second Circuit encompasses New York, Connecticut, and Vermont. Its conclusion that, absent an explicit action by a state legislature, a state and its local governments may invoke copyright protection provides an important shield for privacy if properly applied by New York State and its localities.[276] An examination of the Connecticut FOIA reveals no express abrogation of copyright authority for Connecticut or its localities. Consequently, databases and systems, such as a locally created GIS, should be subject to copyright protection, in order to give the local jurisdictions control of subsequent dissemination of the information. Commercially developed recreation management systems are likely protected by the developer's copyright. Because some customization occurs with each user, and thus some elements of originality are added, the local government's recreation management database is likely copyrightable as a derivative work.[277]

[91] Local governments can take an additional step by employing digital rights management (DRM) technology and placing a copyright management system, a digital "fence," around the data given to a requestor. As described by one commentator, digital rights management

[273] *Id.*
[274] *Id.* at 193.
[275] *See supra* notes 69-72 and accompanying text.
[276] *County of Suffolk*, 261 F.3d at 195.
[277] 17 U.S.C. § 103 (2000).

technology employs digital technology to give copyright owners control over the use of their protected work:

> DRM software prevents purchasers and third parties from making unauthorized uses of digital works. DRM technology has two separate functions. First, it identifies digital versions of copyrighted works. . . . Copyright owners use two main types of existing technologies, known as "watermarking" and "fingerprinting," to create digital identifications for their works. . . . Second, DRM software may also provide copyright owners with control over the various excludable rights of copyright ownership, including . . . the ability to make copies of and redistribute the work.[278]

At least in the Second Circuit, the *County of Suffolk* decision, by concluding that state and local governments can enforce copyright protection,[279] appears to permit states and localities to employ digital rights management technology to protect their copyrights.

[92] Digital fences, however, can be broken. If a digital fence is used to protect the copyright or to prevent manipulation of the data, then the Digital Millennium Copyright Act (DMCA) provides some limited protection.[280] The requester would have legitimate access if given a copy of the information protected by a DRM system. Because of fair use considerations, a person with legitimate access does not violate the DMCA by seeking to break through the digital fence. Assisting someone who attempts to duplicate the data, however, would subject the person assisting to the penalties of the DMCA.[281]

---

[278] Daniel Benoliel, Comment, *Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology*, 92 CAL. L. REV. 1069, 1084-85 (2004) (internal citations omitted).

[279] *County of Suffolk*, 261 F.3d at 195.

[280] Digital Millennium Copyright Act, 17 U.S.C. §§ 512, 1201-1205, 1301-1332 (2000); 28 U.S.C. § 4001 (2000) (governing assumption of contractual obligations related to transfers of rights in motion pictures). For a detailed analysis of the applicability of the DMCA, *see* David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673 (2000).

[281] Digital Millennium Copyright Act, 17 U.S.C. §§ 512, 1201-1205, 1301-1332 (2000); 28 U.S.C. § 4001 (2000). Such a use of the DMCA could create strange bedfellows, with

[93] It is not altogether clear that the requirements of the New York FOIL and the Connecticut FOIA that records be provided in electronic format[282] prohibit the states or their localities from placing a digital fence around the data even if it is not protected by copyright. Although the DMCA penalties would not be applicable, such a step would at least make data matching and related activity more difficult.

V. CONCLUSION

[94] States and local governments are rushing headlong into the digital age, in most instances heedless of the impact upon the privacy of residents. Justice Brennan warned almost 30 years ago that data in electronic form "vastly increase[s] the potential for abuse of that information."[283] These advances into the digital age are occurring in the context of open government laws enacted almost 40 years ago. Consideration of the information privacy concerns and rights of residents is barely on the radar screen of public officials; yet commercial entities, mischief makers, and evildoers are well aware of the opportunities presented.

[95] A RAND study published several years ago commented upon the significance of privacy considerations in e-commerce:

> Privacy is considered by industry as a nice-to-have but not need-to-have feature of E-commerce. If customers demand it, companies will supply–not necessarily enthusiastically (after all, customer lists have resale value), but willingly enough. But the onus on this side of the Atlantic is on the customer's caring enough about privacy to make it an important factor…."[284]

---

privacy advocacy groups joining the entertainment industries in support of some of the more controversial provisions of the Act.

[282] *See* CONN. GEN. STAT. §1-211(a) (2003); N.Y. PUB. O. LAW § 88 (Consol. 1999); Brownstone Publishers, Inc. v. New York City, 550 N.Y.S. 2d 564 (1990) (in response to FOIL request by publishing company, New York City Department of Buildings ordered to provide records on computer tape rather than hard copy).

[283] Whalen v. Roe, 429 U.S. 589, 607 (1977) (Brennan, J., concurring).

[284] LIBICKI, ET. AL., *supra* note 71, at 101.

Similarly, in the public sector, residents need to be increasingly educated regarding the impact of the lack of attention to privacy upon their lives, and must press state legislatures to make needed adjustments to decades-old FOILs. The framers of the FOILs undoubtedly did not intend to jeopardize the lives and fortunes of the residents of their states but, as a consequence of technological inversion, that is the present consequence of the FOILs as they are now applied.[285] As sports coaches often say, let us "return to the fundamentals."[286] The underlying purpose of FOILs is to shed light on "the process of government decision-making" and, concomitantly, to make available documents and statistics "leading to determinations."[287] This purpose is not advanced by forcing the release of databases containing personally identifiable information about residents that has been accumulated to enable the government to function with greater efficiency. FOILs should be limited to advancing their fundamental purpose and should recognize the privacy concerns of residents. Unfortunately, it likely will take a major tragedy to focus the attention of the state legislatures upon these changes.

[96] In the interim, residents need to assert their constitutional and statutory rights to informational privacy aggressively. In addition, they must press their local governments to address privacy concerns and to focus on privacy as an important priority. At a minimum, local governments should designate chief privacy officers. The diffusion of responsibility for addressing privacy matters leaves no one responsible and does not force public administrators to take privacy concerns into consideration. The consequences of lack of attention to information

[285] As Justice Brandeis admonished:

> Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in the insidious encroachment by men of zeal, well-meaning but without understanding.

Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting) (internal citations omitted).

[286] D. Orlando Ledbetter, *Game Day SEC,* ATLANTA JOURNAL-CONSTITUTION, Oct. 30, 2004, at E16.

[287] *See, e.g.*, N.Y. PUB. OFF. LAW § 84 (Consol. 2005). *See supra* note 120 and accompanying text.

privacy by state and local governments will lead to an increase in criminal activity facilitated by anachronistic laws and policies.