January 2000

Public Data and Personal Privacy

Steven C. Carlson
Ernest D. Miller

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/chtlj/vol16/iss1/4

This Comment is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
Public Data and Personal Privacy

*Steven C. Carlson* and *Ernest D. Miller*

**TABLE OF CONTENTS**

I. Introduction ................................................................. 84

II. Architectural Transformations: Databases to Data Networks .......... 85

III. Personal Interests in Public Data ......................................... 86

   A. Notions of Privacy ...................................................... 86
   B. Qualitative Differences in Data ....................................... 87
   C. Distinctions Among Data Recipients ................................. 88

IV. Channels of Disclosures ................................................ 88

   A. FOIA ........................................................................... 88
      1. Goal of FOIA: Transparency of Government ...................... 89
      2. Tension With Privacy Interests .................................... 89
      3. Ad Hoc FOIA Exemptions .......................................... 92
      5. FOIA and the Internet ............................................ 94
   B. Non-FOIA Disclosures .................................................. 96
      1. Driver’s License Data ............................................... 96
      2. The Federal Driver’s Privacy Protection Act .................... 97
      3. Connecticut’s Driver’s Privacy Protection Act .................. 98
      4. Unauthorized and Downstream Uses of Data ..................... 99
      5. Data Origination Versus Data Verification ....................... 100
   C. Interagency Transfers .................................................. 101
      1. Benefits of Data Matching ......................................... 101

---

*1 Law Clerk to the Honorable Roderick R. McKelvie, U.S. District Court for the District of Delaware; J.D., Yale Law School, 1999; B.A., Reed College, 1993.*

*2 J.D. anticipated, Yale Law School, 2000; B.S., Naval Academy, 1990. The authors would like to thank the following people for their assistance and insight with this paper: Professor Jack Balkin, Professor James Boyle, Mitchell Pearlman, Professor Lillian BeVier, Shelly Geballe, Janice Greundel, John D. Woodward, Jr., David W. Marston, and the Honorable Roderick R. McKelvie.*
I. INTRODUCTION

Federal, state, and local governments are currently pursuing ambitious programs to upgrade and integrate their information technology systems into unified data networks. These proposals promise to make vast holdings of data far more accessible to government officials and to the general public. The rapid advance of technology, however, proceeds upon a framework of privacy regulations designed for the insular information systems of the past. The thesis of this paper is that advances in information technology are outpacing the law’s protections for personal privacy, and that new safeguards for privacy, due process, and substantive rights need to be incorporated into law to meet the challenges brought on by heightened access to personal data.

This paper focuses extensively on privacy issues in the State of Connecticut. Connecticut has proposed a massive program to overhaul the isolated databases of its various agencies and transform them into an integrated state-wide data network. Connecticut’s proposal, originally intended to be executed through a $1.5 billion privatization contract, is now slated to proceed under the auspices of the state’s Department of Information Technology (DOIT).1 This paper considers in detail the way in which the proposed technical changes will require that new privacy protections be incorporated into law.

Part I of this paper highlights current trends in information technology, with an in-depth focus on the Connecticut initiative to integrate and privatize its information services. Part II provides a framework for considering the privacy interests of individuals in public data, and the qualitative distinctions among different means of disclosures. Part III, the primary thrust of the document, provides a detailed description of the various channels of information disclosure, including Freedom of Information Act (FOIA) disclosures, non-FOIA

disclosures, and interagency disclosures.

II. ARCHITECTURAL TRANSFORMATIONS: DATABASES TO DATA NETWORKS

Government agencies have commonly stored data in isolated systems before attempting to integrate it into more global systems. The State of Connecticut, for example, long relied on multiple, isolated computer systems within a given agency. It has repeatedly consolidated portions of its information technology systems, either unifying the databases of individual agencies, or creating computing environments shared by a small number of government entities.

A current trend in information technology is to link the databases of government agencies into jurisdiction-wide networks that allow for the common holding of data. These “common information repositories” may be housed at various levels of the network, such that certain information may be accessible at the state level, other information can be obtained at a more limited enterprise level, and other information would be restricted to an agency-specific level. Information is organized at state, enterprise, or agency levels as dictated by concerns about security, management responsibility, and access requirements. The “Statewide INFOstructure,” that is being created in Connecticut, connects agencies to one another and reduces the redundancy and cost of more traditional database management systems.

The transformation to an integrated, jurisdiction-wide data network requires that value judgments be made about the privacy concerns of individual bits of information. By assigning data to a more general level of access, the state can reduce the redundancy of data collection as well as the associated costs of maintaining separate databases. Simultaneously, the state makes personal information more available to government officials, as well as to the public.

The State of Connecticut is currently pursuing a massive proposal to overhaul its information technology services and create this Statewide INFOstructure. The state engaged in extensive

---

3. See id., fig.2-3.
4. See id., fig.3.
5. See id.
6. See id.
7. See id.
negotiations with a private firm to outsource the project for an estimated cost of $1.5 billion over seven years. Negotiations terminated in June 1999 over pricing and labor disputes, but the state has resolved to continue with the program through its internal Department of Information Technology. If successful, this massive undertaking will revolutionize data handling practices in Connecticut and set a standard for the remainder of the states. Since it is taking a leadership role with its privatization plan, Connecticut must address privacy issues from the start to ensure that privacy protections are hardwired into the architecture that is ultimately selected.

Connecticut's plan, while technically ambitious, proceeds upon a set of data privacy laws designed for the insular systems of the past. The privacy protection provided by the legislation that enabled the privatization initiative are based upon existing privacy laws, with no attempt to modify the state's data laws to confront the challenges posed by improved technology. Existing law primarily addresses the release of discrete amounts of sensitive data to the public, and does not account for interagency disclosures and disclosures of aggregations of data that will be made possible as advances in technology permit the integration of public data in a unified data network.

III. PERSONAL INTERESTS IN PUBLIC DATA

Individuals have a number of different personal interests in the information the government holds. While the term "privacy" may be generally ascribed to all of these interests, they can be differentiated into more particular concepts.

A. Notions of Privacy

One kind of privacy interest that individuals have is an interest in personal security and safety. Access to government data can facilitate the misdeeds of others by making available potential victims' personal information, such as their addresses, Social Security numbers, and medical records. The harm is ultimately not one of

8. See Daly, supra note 1.
9. See id.
11. For example, actress Rebecca Shaeffer was shot and murdered when a lunatic fan acquired her address through the motor vehicle records held by the State of California. See W. Kent Davis, Drivers' Licenses: Comply with the Provisions of the Federal Driver's Privacy Protection Act; Provide Strict Guidelines for the Release of Personal Information from Drivers' Licenses and Other Records of the Department of Public Safety, 14 Ga. St. U. L. Rev. 196, 196
privacy, but of other more serious and even criminal offenses that can be committed easily through access to personal data.

Second, individuals have due process interests in the proper handling of their data. As discussed below, government agencies are increasingly sharing public data between themselves. While such data exchanges can be a boon to governmental efficiency, they increase the risk that officials will act on erroneous data. Absent independent checks to verify the authenticity of matched data, agencies risk depriving individuals of their due process rights when they take adverse action based upon erroneous data.

Third, individuals have more abstract interests that are best described by the term “informational privacy.” This term defies an easy definition, but it may be generally described as the desire of individuals to limit the kinds of information that others know about them. Informational privacy interests extend beyond concrete harms to personal security or safety, and implicate those disclosures of personal data that simply reveal information that would not otherwise be known.

B. Qualitative Differences in Data

Governments collect a vast array of personal data. Some data, such as tax and medical records, are extremely sensitive and have long been recognized as sources of concern for the privacy interests of individuals. Other sources of personal information are quite innocuous when considered in discrete amounts, although they can be compiled and matched to create broader profiles of individuals that are invasive of personal privacy. Because governments hold a spectrum of data about their citizens, public databases are especially attractive sources of information for people seeking to generate information profiles of others.\(^1\)

\(^{12}\) This information includes voting records, motor vehicle records, public housing records, records relating to professional and recreational licenses, schooling records, unemployment records, library circulation records, and divorce records.
C. Distinctions Among Data Recipients

Governmental disclosures of personal information can also be differentiated according to the identity of the recipient. Personal data is often disclosed by governments to the general public. Information may also be disclosed among government entities, either within a given jurisdiction, or between jurisdictions. This practice is becoming increasingly common with the creation of integrated data networks.

The differences between sensitive and profiling data, and between governmental disclosures to the public and governmental disclosures among government agencies give rise to four general categories of governmental disclosures: (I) disclosure of sensitive data to the public; (II) disclosure of profiling data to the public; (III) disclosure of sensitive data between government entities; and (IV) disclosure of profiling data among government agencies. Most laws have focused upon the first kind of disclosure, with states having elaborate regulatory schemes designed to restrict the disclosure of sensitive data to the public. As advances in technology increasingly permit the release of profiling data to the public and the disclosure of sensitive data among government agencies, existing data laws will provide less of a measure of security for the privacy interests of individuals.

IV. CHANNELS OF DISCLOSURES

The replacement of isolated databases by integrated data networks stands to lead to a dramatic increase in the quantity of personal data that is disclosed by the state, both to the public and to other governmental agencies. This Part will detail the existing channels by which governments disclose personal data, and will describe the likely impact of new information technology systems upon the nature of such disclosures.

A. FOIA

State and federal governments are mandated to disclose records to the public pursuant to the freedom of information acts (FOIAs) of their respective jurisdictions. FOIAs commonly have three components. First, they provide that all records maintained or kept by public agencies shall be public records available for public inspection or copying. Second, they create categories of exemptions, such that exempted records are not required to be disclosed. Third, they stipulate how non-exempt public records are to be disclosed to the
public. FOIAs will be sharply impacted by current developments in information technology. As advances in data management systems improve access to public records, far greater amounts of personal information stand to be disclosed to the public.

1. Goal of FOIA: Transparency of Government

Every state, as well as the federal government, has its own FOIA that dictates the scope of information that is open to public inspection. The goal of FOIAs is to promote efficiency and fairness in government by rendering it transparent to the citizenry. The Supreme Court has stated that “[t]he basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed.” James Madison articulated the basic principles behind FOIAs when he stated that “the right of freely examining public characters and measures, and of free communication thereon, is the only effectual guardian of every other right.” FOIAs have repeatedly served as important tools to expose bad practices of government.

2. Tension With Privacy Interests

FOIAs have prompted a decades-long, well-chronicled tension between the goals of public disclosure and the privacy interests of individuals. FOIAs create a presumption that all public records, including those containing personal information, shall be available for public inspection. Records can only be withheld from public disclosure upon a determination that the information falls within one or more of the enumerated FOIA exemptions. These exemptions are frequently construed narrowly to give full effect to the goal of providing full disclosure of records relevant to the public interest. Connecticut is no exception. The Connecticut Supreme Court has repeatedly ruled that “the general rule under the Freedom of

---

13. For a compilation of various privacy laws from all fifty states, see Bruce D. Goldstein, Comment, Confidentiality and Dissemination of Personal Information: An Examination of State Laws Governing Data Protection, 41 Emory L.J. 1185 (1992).
17. See, e.g., CONN. GEN. STAT. ANN. § 1-210(a) (West Supp. 1999).
18. See, e.g., CONN. GEN. STAT. ANN. § 1-210(b) (West Supp. 1999).
Information Act is disclosure with the exceptions to this rule being narrowly construed. The burden of establishing the applicability of an exemption clearly rests upon the party claiming the exemption.\textsuperscript{19}

The Connecticut FOIA exempts disclosure of "[p]ersonnel or medical files and similar files the disclosure of which would constitute an invasion of personal privacy."\textsuperscript{20} Connecticut courts, however, have construed this exemption narrowly and have permitted disclosure of personal data when legitimate public interests can be advanced through disclosure of contested records. Personnel and medical files, for example, can be withheld from disclosure only when "the information sought by a request does not pertain to legitimate matters of public concern and is highly offensive to a reasonable person."\textsuperscript{21} Records relating to public employees are presumptively matters of public concern, and courts frequently override the personal information exemption of FOIA in order to disclose information about how public agencies function.\textsuperscript{22}

The Connecticut Supreme Court found that society's interests in institutional transparency trump personal privacy interests in the context of tax delinquency records. In State v. Freedom of Information Commission, the Court mandated that tax delinquency records be disclosed to the public.\textsuperscript{23} Tax records are ordinarily covered by stringent privacy protections.\textsuperscript{24} The court, however, ruled that tax delinquency lists, which contain the identity of the debtors and the amount of their delinquencies, are public records. The court noted that the public has a strong interest in "knowing whether the burden of public expenses is equitably distributed and whether public employees are diligently collecting delinquent accounts."\textsuperscript{25}

The Connecticut FOIA has also trumped privacy protections in the legislature. In 1976, Connecticut enacted a global privacy law that prohibited disclosure of personal data absent an individual's permission.\textsuperscript{26} The law contained few exceptions,\textsuperscript{27} and it granted a

\textsuperscript{21} Perkins, 635 A.2d at 791.
\textsuperscript{22} See, e.g., id.
\textsuperscript{26} See \textsc{Conn. Gen. Stat. Ann.} § 4-191 (1977 & West Supp. 1998) (repealed 1979) ("No agency or any of its employees shall disclose or transmit any personal data to any other individual, corporation or municipal, state, or federal agency without the consent of the person, except as provided in enumerated exceptions.").
private right of action to individuals whose data were wrongfully disclosed.\textsuperscript{28}

The personal data law, however, clashed with the goals of the Connecticut FOIA. Whereas the Connecticut FOIA mandates that personal information, with narrow exemptions, be disclosed to the public, the personal data law created a private right of action against agencies that disclosed such information. Agencies found themselves legally liable under the personal data law for conduct they were required to perform under the Connecticut FOIA.\textsuperscript{29} Recognizing the inherent tension between the personal data law and the state's FOIA, the Connecticut legislature repealed the personal data law.\textsuperscript{30} Mitchell Pearlman, the present Executive Director of the Connecticut Freedom of Information Commission, was actively involved in the 1979 repeal of the personal data law, and states that the two sets of laws were antagonistic and impossible to mutually enforce.\textsuperscript{31} Privacy laws in Connecticut are now limited to certain procedural safeguards,\textsuperscript{32} the privacy exemption of state's FOIA,\textsuperscript{33} and miscellaneous privacy provisions that are scattered throughout the general statutes as discussed below.

FOIAs establish a bias in favor of disclosure of information to the public, particularly in Connecticut. Connecticut's FOIA imposes enforceable legal liability upon agencies that do not disclose their public records. Powerful interests often seek disclosure of public records through Connecticut's FOIA, and frequently litigate their claims when agencies deny disclosure. To block disclosure of privacy-related records, the burden falls on the agency to show that the record falls within the personal information exemption to the state's FOIA. Not only must the agency show that the record qualifies as a "personnel or medical or similar file["," but the agency must also demonstrate that the privacy interests at stake outweigh the public interest in disclosure, and that the disclosure would be "highly

\textsuperscript{27} The exceptions to the privacy law were limited to intra-agency disclosures, disclosures necessary to prevent physical harm to the data subject, disclosures otherwise permitted by statute, and disclosures made pursuant to subpoena. See \textsc{Conn. Gen. Stat. Ann.} § 4-191 (1977 & West Supp. 1998) (repealed 1979).
\textsuperscript{29} Telephone interview with Mitchell Pearlman, Executive Director, Connecticut Freedom of Information Commission (March 18, 1999) (on file with authors).
\textsuperscript{30} Public Act No. 79-538, 1979 Conn. Acts 79-538 § 2 (Reg. Sess.).
\textsuperscript{31} Pearlman interview, supra note 29.
offensive” to a reasonable person. Since there is often a presumption in favor of disclosure, the withholding agency has a strong burden to overcome. Moreover, there are no global privacy laws in Connecticut that impose affirmative limits on the disclosure of personal data. Additionally, agencies may be particularly prone to disclose personal data since the individual concerned is generally not a party to the FOIA dispute. These factors create an institutional bias in favor of disclosing personal information to requesting parties.

3. Ad Hoc FOIA Exemptions

As discussed above, the Connecticut FOIA has a general privacy provision written into the heart of the act. The provision exempts “personnel and medical and similar files” from the disclosure requirements of the act when their disclosure “would constitute an invasion of personal privacy.” The state legislature commonly reconfigures the scope of the state’s FOIA by adding exemptions for some records or by expressly relegating other classes of information to the public domain. These provisions are scattered throughout the provisions of the Connecticut FOIA, resulting in a patchwork quilt of privacy provisions. Although the general privacy provision quoted above is useful as a starting point for addressing various privacy disputes, the real scope of the Connecticut FOIA is determined by hundreds of individual provisions that spell out in detail what records may be subject to public disclosure. Many of these laws are catalogued in the appendix.

The language of the various provisions suggests the political nature of the Connecticut FOIA. While the names of the holders of most professional and recreational licenses are fully subject to disclosure, Connecticut law makes a number of exceptions. Holders of licenses for firearms and assault weapons, for example, receive an exemption. Information about the activities of hunters, trappers, and commercial fishermen also receives special protection. In contrast, personal data is fully disclosed for sex offenders. The State of Connecticut makes available the names, addresses, photos, and

34. See Perkins, 635 A.2d at 787, 790.
35. See id. at 790.
criminal histories of resident sex offenders, all searchable on the Internet.40

For certain classes of data other than personnel and medical data, the legislature goes beyond the protections afforded by routine Connecticut FOIA exemptions and adds additional provisions that further restrict the legality of disclosing the data. Performance evaluations of judges, for example, are afforded utmost protection. Any information disclosed to members of the judicial department is to be used by such members “only for the purpose for which it was given and shall not be disclosed to any other person.”41 More than merely prohibiting disclosure of the data to the public, as does a normal FOIA exemption, this provision prohibits the disclosure of the data to anyone outside the judicial evaluation committee.


The first step of the Connecticut FOIA, as discussed above, is to divide the universe of public information into exempt and non-exempt records. The second step of the Connecticut FOIA is to make the non-exempt records available to the public. This latter step is being revolutionized by current advances in information technology services.

The Connecticut FOIA has traditionally provided for two methods of disclosing non-exempt records to the public. Citizens can inspect and photocopy public records at the site of the agency holding the information. This method imposes obvious burdens of time, travel, and money upon requesting individuals. Alternatively, requesting parties can obtain Connecticut FOIA releases by correspondence. A requesting party can mail a request to the Freedom of Information Commission (FOIC), stipulating what information is desired. This method of disclosure can be particularly cumbersome, however, if the requestor does not know precisely which documents she seeks. Moreover, this process is expensive. Connecticut law permits charges of $0.25 (for state agency information) or $0.50 (for local government agency information) per page photocopied. Expansive searches can be quite costly, both in terms of time and money. These transaction costs, undesirable as


they are, create an artificial barrier that restrains the disclosure of personal data. Legally non-exempt personal data becomes suppressed, de facto, when the transaction costs of disclosure are considered.

5. FOIA and the Internet

Advances in information technology will revolutionize the mechanics of FOIA disclosures. The State of Connecticut is currently in the process of uploading many of its public records onto the Internet. Connecticut's registry of convicted sex offenders, for example, is freely accessible on-line, and can be searched by name, town, or zip code.

Questions immediately arise as to what type of information and how much information should be uploaded onto the Internet. If the courts or the legislature have ruled that a category of records is subject to FOIA, then what justification remains for preventing the records from being posted? Is there a public interest in maintaining the existing slow and tedious system for processing FOIA requests? Arguably, the slowness of the present system is one of the best safeguards for the privacy interests of individuals.

If FOIAs are interpreted as a mandate to upload all non-exempt records onto the Internet, then the primary effect of FOIAs will diverge from their original goal of promoting transparency of government. FOIAs will increasingly serve to bring other people's public action and inaction to public light. For example, tax delinquency records, as discussed above, have been construed in Connecticut to be non-exempt public records for the purposes of the state's FOIA. The state can promote the transparency of government by posting tax delinquency records on the Internet to air its tax enforcement practices and to show that its policies are fair and non-discriminatory. The predominant effect of such use of the Internet is likely to be the social stigmatization of those who are delinquent in paying their taxes. If the public data is valid and an individual is truly delinquent in his taxes, then perhaps society will benefit by having such an electronic forum. Fear of being recognized by one's neighbors as a tax evader may be a better means of ensuring equitable tax collection than by relying on government enforcement.

43. See supra note 40.
45. See generally ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS
Posting non-exempt public records on the Internet can abridge people’s interest in informational privacy. People may understandably want their public actions to remain anonymous. Whether society should recognize this interest in anonymity is a difficult question. People generally hold an interest in having a blank slate and starting fresh in the wake of past mistakes. If all public information is posted on the Internet, this will serve to create a permanent record that will mark people for life, depriving them of an opportunity to restart their lives with a blank slate. It is unclear the extent to which society should recognize individuals’ interests in leaving their public actions anonymous. This information has been deemed by the courts and the legislature to be a matter of public record, so why should it be only accessible through the cumbersome mechanics of today’s FOIA procedures? The challenge is to discern whether the state should recognize notions of informational privacy such that certain non-exempt records should be withheld from the Internet. To do so, the state may craft, as it has done in the past, ad hoc exceptions to the general rule in favor of posting non-exempt records on-line. This can be an effective means of preventing the posting of discrete collections of information, but this method runs the risk of granting special treatment to politically favored groups. Alternatively, the courts and legislature can attempt to redraw the line between exempt and non-exempt records to discourage disclosure of personal data. This approach may be problematic, however, in that it will require the reformulation of decades of case law, and will suppress the release of certain information that has been heretofore available under FOIAs. Neither approach is desirable, and the best policy may be to make all non-exempt records available over the Internet.

If all non-exempt records are posted on the Internet, various procedural safeguards need to be implemented to ensure that the publicly posted information is both current and accurate. People should be informed when their personal data is to be posted on the Internet and should have the opportunity to correct any false or misleading information. Government, moreover, should be required to purge old data that is not essential to its mission. These procedural rules have long been part of Connecticut law, having survived the repeal of Connecticut’s personal data law.\footnote{See Conn. Gen. Stat. Ann. § 4-193 (1998 & West Supp. 1999).} Adherence to these

\footnote{SETTLE DISPUTES (1991) (asserting that social coercion can be more effective than legal coercion).}
provisions is of critical importance as personal data becomes ever more widely available in the digital age.

B. Non-FOIA Disclosures

Federal and state governments engage in many disclosures of personal data that cannot be justified under FOIA. These disclosures are not seen as a way to promote the transparency of government, but rather as a means to facilitate private-sector interests. By making available useful data that would only be available on a piecemeal basis through other sources, governments can reduce transaction costs of private-sector endeavors. Such disclosures do not promote efficiency or fairness of government and are frequently made without any involvement by the Freedom of Information Commission.\(^4\) Rather, these disclosures are made by individual agencies pursuant to deliberate policy choices as a means of facilitating private-sector interests.

The public stands to benefit from such disclosures insofar as private services can be made more readily available. Privacy concerns, however, are readily apparent. While individuals are often required to submit personal information to the government, they generally lack the authority to prevent the government from disclosing their personal data.

1. Driver's License Data

Most state motor vehicle departments sell, or otherwise disclose, driver's license data to private-sector interests.\(^48\) These data include people's names, addresses, Social Security numbers, and photographs.\(^49\) The State of Wisconsin, for example, generates roughly $8 million annually from the sale of driver's license data.\(^50\) The State of Indiana sells driver's license data, along with motor vehicle registration records and other information, directly over the Internet.\(^51\) Driver's license records and registration records cost $5.00 a piece.\(^52\)

\(^48\) See Travis v. Reno, 163 F.3d 1000, 1002 (7th Cir. 1998).
\(^49\) See CONN. GEN. STAT. ANN. § 14-10 (West Supp. 1999).
\(^50\) See Travis v. Reno, 163 F.3d 1000, 1002 (7th Cir. 1998).
\(^52\) See id. To comply with Indiana privacy law, requestors must click upon a category of permissible uses for the data, although it is not clear if there is any way to monitor the use of the
The sale of driver’s license data provides a revenue source that can help state agencies adopt streamlined information technology systems that are useful to the general public. Arguably, the opportunity to generate revenue through the disclosure of driver’s license data provides an incentive for states to improve their telecommunications systems and make services available to the general public.

The practice of selling driver’s license data, however, raises serious privacy issues that have engendered strong opposition and congressional rebuke. Many people do not want their residential information listed in public directories. People have a legitimate interest in having their residential information kept separate from the public sphere and commonly forego being listed in public directories. This privacy interest may simply be one of not wanting others to know where they live, or may be more deeply rooted in concerns for personal security and safety. People lose this privacy interest when state motor vehicle departments disclose driver’s license data absent individuals’ consent.

2. The Federal Driver’s Privacy Protection Act

State disclosures of driver’s license data received substantial press in light of the violence facilitated by their release. A California actress, Rebecca Schaeffer, was murdered at her home after a lunatic fan procured her address through the local department of motor vehicles. In response, Congress passed the Driver’s Privacy Protection Act (DPPA), which has been replicated in Connecticut and in other states nationwide.

The federal DPPA prohibits unrestricted disclosures of driver’s license data, but preserves the ability of state motor vehicle departments to serve as clearinghouses of information for third parties. The DPPA creates a broad prohibition on disclosure of personal data contained in motor vehicle records to any person or entity. The DPPA then enumerates permissible uses of such data. Many of the enumerated uses pertain to issues of motor vehicle safety and theft. Other uses are far broader in scope. The DPPA, for

---

53. The Indiana system, for example, provides an information framework for public services throughout the state. See id.
54. See Davis, supra note 11, at 196.
example, permits the disclosure of driver's license data to any public official for use in carrying out public functions. The DPPA also allows disclosure of data to private firms "in the normal course of business" to verify or correct existing data. In addition, the DPPA permits state motor vehicle departments to disclose their data for bulk distribution of marketing surveys and solicitations if individuals have an opportunity to opt-out. The permissible uses enumerated in the DPPA leave the law, in the wording of the Eleventh Circuit, "riddled ... with more holes than Swiss cheese." The DPPA is dubiously enforceable, moreover, as circuits are split on whether the DPPA is an impermissible encroachment on state sovereignty.

3. Connecticut's Driver's Privacy Protection Act

The DPPA, and its state law analogs, may serve to lull citizens into thinking that their personal data will be shielded from disclosure. The Connecticut DPPA requires that all applicants for drivers permits have the opportunity to prevent their driver's license information from being disclosed. All such applications must contain the following notice:

NOTICE: Personal information collected by the Department of Motor Vehicles may not be disclosed to any person making a request for a motor vehicle record in accordance with the provisions of subsection (c) or (d) of section 14-10 of the general statutes unless you indicate your consent to disclosure. Do you wish to allow disclosure under such circumstances? Yes ( ) No ( )

On its face, this notice appears to assure people that their driver's license data will remain secure from disclosure. Indeed, absent the driver's consent, the Connecticut Department of Motor Vehicles is prohibited from disclosing the data to most people who appear at the Department in person. The notice, however, does not allude to the fact that, despite the refusal of license applicants to permit disclosure of their data, the Department remains free to disclose their personal

---

64. Id.
65. See CONN. GEN. STAT. ANN. § 14-10(c), (d) (West Supp. 1999).
data pursuant to subsections (e) and (f) of the driver’s license statute. These subsections authorize the Department to disclose the data for the litany of uses permitted by the Connecticut DPPA.

The Connecticut driver’s license statute is misleading and it masks the privacy policies of the state. The Connecticut legislature has made a deliberate policy choice to permit personal information to be disclosed in order to advance certain interests that, perhaps, inure to the benefit of the general public. The state also generates revenue through these disclosures. This policy choice, if properly aired, can possibly be justified. However, the manner by which the state effectuates its policies is deceptive. By asking people if they would consent to the disclosure of their personal data, and then disclosing it regardless of their responses, the state flaunts the trust of its citizens. The disclosures do not advance goals that have been openly endorsed by the public. Nor do such disclosures promote government efficiency and fairness, as do FOIA disclosures. With the release of these records, the State of Connecticut unjustifiably discloses important personal information—including names, addresses, Social Security numbers, and photographs—despite the express refusal of its citizens.

4. Unauthorized and Downstream Uses of Data

Additional problems arise when publicly held information is disclosed clearinghouse-style. States may agree to disclose personal records in bulk for express and legitimate purposes. The records that are disclosed, however, are valuable, and are readily resold for secondary and unapproved uses. While the DPPA and its state law counterparts set forth stiff penalties for unapproved uses of disclosed records, enforceability is a major problem. Recent incidents involving driver’s license data illustrate the problem of specifying the uses for which disclosures are permitted.

Image Data, a New Hampshire-based company, succeeded in persuading a number of states to sell it copies of their driver’s license photos. Image Data explained that the photos would be used for a nationwide credit fraud prevention system, whereby the images of credit card holders would flash at checkout counters, allowing store clerks to verify customers’ identities. South Carolina sold the company 3.5 million photos for $5000. Florida and Colorado signed similar contracts. The Washington Post then reported that Image Data was funded in part by the United States Secret Service, and that
the photos were to be used to construct a national network to combat terrorism and immigration fraud. Upon this revelation, the governors of Florida and Colorado blocked the sale of photos, and the State of South Carolina sued for the recovery of its records. The states reportedly had never been informed that the photos were to be used for such a system, and had no knowledge that federal officials were involved in the deal. Government data is exploited broadly over the Internet. Companies such as TenantScreening.com employ public data to offer landlords and other parties a method to learn the personal histories of prospective tenants and others. Another company compiles federal, state, and municipal data to provide employers with background checks and other surveillance services for monitoring prospective and existing employees. The reality is that government databases have been widely appropriated by private firms. This public data is being used not as a means for monitoring government, but as a tool for investigating individuals. While the DPPA enumerates the permissible private-sector uses of driver’s license data, no statutory exemption covers uses such as tenant screening and employee monitoring. Clearly, the data used in these surveillance applications have been transferred beyond the limited uses sanctioned by privacy laws.

Non-FOIA disclosures can have valid policy goals. The problem, however, is that data are readily and tacitly resold. Governments have little ability to track downstream sales of data. Given the value of such databases, the rapid transferability of the records, and the difficulty in tracking the subsequent uses, governments should assume that downstream resale of personal information will occur, and should generally refrain from disclosing the information except for compelling purposes.

5. Data Origination Versus Data Verification

Solutions do exist to help reconcile people’s interest in

---


67. See id.; see also Robert O’Harrow Jr., *South Carolina Cuts Ties to Driver Database*, WASH. POST, Mar. 23, 1999, at E3.


informational privacy with society’s broader interest in facilitating transactions. The problem with the current system for disclosing driver’s license records is that the disclosures are broader than need be to effectuate the goals of the DPPA. For example, the DPPA permits states to use driver’s license data to verify third parties’ data.\textsuperscript{71} States, however, need not disclose any personal data to fulfill this role. It would be sufficient for the state to establish a data verification system, possibly electronically, that would allow third parties to check the authenticity of individual’s representations. No information would be released by the state other than a yes/no answer as to whether the requestor’s information is correct. In the event the data do not coincide, this system would provide a preliminary notice to the requesting party that the individual’s data do not match public filings, and that further inquiry as to the authenticity of the individual’s representations may be necessary. No information would be disseminated to third parties, and the anonymity interests of individuals would be protected.

C. Interagency Transfers

The current trend of database integration stands to revolutionize current practices of information sharing between governmental agencies. Governments can realize substantial improvements in efficiency through data sharing by reducing the redundancy of data collection and by preventing fraud on the government. Conversely, such data sharing practices are likely to impinge on the personal privacy and substantive rights of individuals.

1. Benefits of Data Matching

Governments commonly engage in a practice known as “data matching” to detect and prevent fraud. Connecticut law gives broad discretion to the Department of Social Services (DSS) and its constituent divisions to match its data against the records of other agencies. The DSS, for example, jointly maintains a database with the Labor Department to track the employment contracts of recipients of aid in its family assistance program.\textsuperscript{72} Connecticut law also authorizes the Child Support Enforcement Bureau (Bureau) of the DSS to compare the records that it receives from “deadbeat” parents with the records that are submitted by such parents to other

\textsuperscript{71} See 18 U.S.C.A. § 2721(b)(3)(A) (West Supp. 1999); see also CONN. GEN. STAT. ANN. § 14-10(f)(A), (B), (G) (West Supp. 1999).

\textsuperscript{72} See CONN. GEN. STAT. ANN. § 17b-688b (West Supp. 1999).
government agencies and to private institutions. The Bureau is also mandated to enter into agreements with private financial institutions to develop automated data matching systems to track the deposits of deadbeat parents and submit such information to the Bureau on a quarterly basis. The broad data matching authority of the Bureau derives directly from the federal 1996 Welfare Reform Act, which confers such investigative powers upon the child support agencies of all states.

Governments have improved their fraud detection systems and have generated significant cost savings through data matching programs. The federal Department of Education recovered $3.4 million in delinquent loan repayments by matching its roster of delinquent student loan debtors against records of federal employees. The State of Texas, similarly, recovered over $600,000 in Medicaid overpayments in less than two months through its data matching system. Finally, the Province of Alberta discovers roughly 300 clients a month who overdraw benefits.

2. Privacy Interests in Matched Data

Data matching gives rise to numerous concerns over privacy interests and substantive rights. Privacy concerns generally stem from a fear of the government having unrestricted power to employ its data in the monitoring and surveillance of individuals, and from a notion that the personal autonomy of individuals is violated when their personal data is used for purposes other than those for which the data was originally disclosed. Without a doubt, an individual's interest in informational privacy is in tension with the public interest in accurate decision-making and efficient policy implementation. Thus, the question arises whether governments should be permitted to

---

80. See id.
employ data for unconsented-to uses, and if so, what enforceable restrictions can be placed upon public agencies from sharing data and from taking action based on shared data.

One option would be to prohibit governments from using personal data for unconsented-to uses. To be sure, such prohibitions are in force in certain circumstances. Connecticut imposes strict non-disclosure standards on HIV data and tax return data. But few categories of data spark sufficient public interest to enact laws against intra-governmental data disclosures. In the absence of statutory prohibitions, some privacy advocates nonetheless argue that the government should be prohibited from using data for unconsented-to uses.

This position is untenable. To restate the argument of Professor Lillian BeVier, the government has legitimate interests for engaging in non-consensual uses of personal data that outweigh the privacy interests of individuals whose personal data might be shared. Legitimate interests of the government are clear, as discussed above. Privacy interests of individuals, on the other hand, not only vary widely from person to person, but they often trifle in comparison to the wider goals of the public administration. Professor BeVier suggests that the primary privacy interest sought to be protected by banning such disclosures is to allow people the freedom of informational anonymity. But it is not clear to what extent individuals should be able to restrict public agencies from sharing valid data with other officials. How, if at all, is an individual’s personal autonomy violated when an agency matches its data against motor vehicle records? Should society recognize a privacy interest in “deadbeat” dads attempting to hide their public employment contracts from the child support enforcement bureau? To be sure, there may be an affirmative notion of personal privacy that might be violated when public officials share an individual’s personal data. But when valid data is shared between agencies pursuant to an officially endorsed

83. See Letter from Joseph Grabarz, President, Connecticut Civil Liberties Union, to Steven Carlson and Ernest Miller (Feb. 12, 1999) (on file with authors).
84. See BeVier, supra note 79, at 475.
85. See supra note 76 and accompanying text.
87. See id.
policy, the privacy interest of the individual appears inconsequential.88 As one privacy expert noted, public data systems "would probably fall apart if individuals were to exercise complete control over the use of their personal information."89

Some restraints on data sharing are essential. There is a vast potential for public officials to abuse personal data, and the more that data are transferred between agencies, the greater the risk of harm. Some of the worst incidents of data theft stem from the behavior of public employees with access to sensitive personal information. Mitchell Pearlman, Executive Director of Connecticut's Freedom of Information Commission, feels that the misappropriation by public employees of state data poses one of the greatest hazards to personal privacy.90 In Connecticut, for example, numerous employees of the Labor Department were found to have leaked confidential salary data of the president of the Connecticut Business and Industry Association to embarrass him in the press during a union dispute.91 Workers at the United States Internal Revenue Service have repeatedly been found to snoop on confidential tax data, often selling the information to third parties.92 And, an employee of the Federal Trade Commission was convicted for credit card and mail fraud after accessing files containing personal information and Social Security numbers.93 Many public employees abuse government data, and safeguards must be implemented to constrain the flow of data to legitimate uses.

3. Federal Data Matching Law

Several statutes have been enacted at the federal level to remedy privacy concerns related to data matching. These laws establish important baseline principles for interagency data management at all levels of government. The first major federal law directed towards data privacy was the Privacy Act of 1974 (Privacy Act), which, among other things, established a prohibition on interagency

88. See BeVier, supra note 79, at 476.
90. Pearlman Interview, supra note 29.
92. See Hershey, supra note 11.
disclosure of personal data absent the consent of the data subject.\textsuperscript{94} The Privacy Act, however, has been viewed as a “paper tiger” due to the loopholes that negate its protections.\textsuperscript{95} The most significant loophole to the law is the “routine use” exception, which permits agencies to share personal data when the disclosure is for a routine use. This exception has been construed liberally, permitting transfers for any “necessary and proper” function.\textsuperscript{96}

In response to the apparent lack of controls imposed on interagency transfers by the Privacy Act, Congress enacted the Computer Matching Act of 1988 ("Computer Matching Act").\textsuperscript{97} The Computer Matching Act established a more explicit set of guidelines that govern the ways data may be shared between government agencies, and the extent to which the agencies may take adverse action against individuals based upon shared data. The Computer Matching Act has proven difficult to administer and it is questionable what practical effect it has had on the nature of interagency disclosures.\textsuperscript{98} The Computer Matching Act does, however, establish some fundamental principles of fair information practices that should be adopted at the state level, where many of these issues have not been as thoroughly confronted as within the federal government.

The Computer Matching Act provides for a number of protections that are absent in Connecticut law. First, the Computer Matching Act establishes due process standards that limit the extent to which agencies can act based on matched data.\textsuperscript{99} It recognizes the technical shortcomings of data matching programs, in that data may be improperly inputted, may be wrongly processed, may be outdated and may produce “false positive” matches.\textsuperscript{100} The Computer Matching Act, therefore, prevents agencies from taking adverse action against individuals unless the results of data matches can be corroborated with firsthand data, or if there is a “high degree of confidence” that the matched data is correct.\textsuperscript{101} The Computer Matching Act provides for a number of protections that are absent in Connecticut law. First, the Computer Matching Act establishes due process standards that limit the extent to which agencies can act based on matched data.\textsuperscript{99} It recognizes the technical shortcomings of data matching programs, in that data may be improperly inputted, may be wrongly processed, may be outdated and may produce “false positive” matches.\textsuperscript{100} The Computer Matching Act, therefore, prevents agencies from taking adverse action against individuals unless the results of data matches can be corroborated with firsthand data, or if there is a “high degree of confidence” that the matched data is correct.\textsuperscript{101} The Computer Matching Act provides for a number of protections that are absent in Connecticut law. First, the Computer Matching Act establishes due process standards that limit the extent to which agencies can act based on matched data.\textsuperscript{99} It recognizes the technical shortcomings of data matching programs, in that data may be improperly inputted, may be wrongly processed, may be outdated and may produce “false positive” matches.\textsuperscript{100} The Computer Matching Act, therefore, prevents agencies from taking adverse action against individuals unless the results of data matches can be corroborated with firsthand data, or if there is a “high degree of confidence” that the matched data is correct.\textsuperscript{101} The

\begin{thebibliography}
\bibitem{95} See BeVier, supra note 79.
\end{thebibliography}
Matching Act requires that individuals receive notice when benefits are to be reduced or terminated based on matched data and that they have a 30-day period to contest the findings. This provision is an important safeguard against the wrongful deprivation of an individual's substantive rights and establishes a sensible baseline for the extent to which agencies can conduct their business through data that they did not originally procure.

Second, the Computer Matching Act limits the extent to which data can be transferred between agencies. It provides that data may not be exchanged between agencies unless pursuant to an express matching agreement. Matching agreements, among other requirements, must stipulate the purpose of the planned matches, must describe the records that will be matched, and must establish procedures for notifying individuals if adverse action is to be taken based on computer matches. These provisions attempt to protect the privacy interests of individuals by limiting the number of agencies that can have access to personal data and by requiring that agencies incorporate due process protections into their matching programs.

4. State Data Matching Law

Connecticut has data privacy laws that concern interagency transfers of data. These laws require agencies to keep logs recording when a person's data is disclosed to other agencies and require agencies to permit individuals to inspect, verify and correct personal data being stored by the government. Several important provisions of the Computer Matching Act, however, are absent in Connecticut.

Connecticut law has no provisions analogous to the federal due process protections in data matching programs. As such, agencies are not required to rely on firsthand data before taking adverse action against individuals. As more and more state agencies are interlinked through the proposed state-wide data network, computer matching is becoming an increasingly widespread practice throughout Connecticut's government. It is important that such due process

107. See id.
108. See Letter from James Wietrak, Connecticut Department of Social Services, to Steve Carlson (May 18, 1999) (on file with authors).
protections be written into state data law to ensure that agencies take adverse action only when acting on accurate data.

Connecticut law, moreover, does not mandate that data matching programs be conducted pursuant to formalized matching agreements. To be sure, Connecticut has adopted a number of provisions, either on a general level or an ad hoc basis, that set a foundation for more comprehensive data matching protections. Connecticut law does provide that public records are the property of the procuring agency and shall not be transferred except as authorized by law. The law also grants the Attorney General the authority to recover improper transfers of data between agencies. Connecticut law, however, does not restrict interagency data transfers to those contexts specified under formalized data sharing agreements, as mandated at the federal level.

Connecticut’s tax laws indicate the weaknesses of the state’s information technology systems and point to the need for restraint in the use of data matching programs. State law allows the Tax Commissioner to transfer tax records to other governmental agencies for various purposes. The Tax Commissioner, however, retains the discretion to refuse to transfer individuals’ tax records when he or she perceives that the receiving agency lacks adequate safeguards for protecting the information. The statute is remarkably detailed in the extent to which it stipulates the protections that the Tax Commissioner may require to be in place before records are transmitted. Tax data are arguably some of the most important data

113. The statute, provides, in pertinent part that the Commissioner may refuse to disclose tax records to any agency unless such agency or office shall have:
(1) Established and maintained, to the satisfaction of the commissioner, a permanent system of standardized records with respect to any request, the reason for such request, and the date of such request made by or of it and any disclosure or inspection of returns or return information made by or to it; (2) established and maintained, to the satisfaction of the commissioner, a secure area or place in which such returns or return information shall be stored; (3) restricted, to the satisfaction of the commissioner, access to the returns or return information only to persons whose duties or responsibilities require access and to whom disclosure may be made under this section or by whom inspection may be made under this section; (4) provided such other safeguards which the commissioner prescribes as necessary or appropriate to protect the confidentiality of the returns or return information; (5) furnished a report to the commissioner, at such time and containing such information as the commissioner may prescribe, which describes the procedures established and utilized by such agency or office for ensuring the confidentiality of returns and return information required by this subsection; and (6) upon completion of use of such returns or return information, returned to the commissioner such returns or return
held by the state and it is no surprise that highly restrictive policies are in place with respect to the transfer of such records. The thoroughness of the laws covering transfers of tax data, however, suggests that the government’s data sharing programs in other contexts are less secure.

Data matching programs, when properly administered, can be a boon to the efficiency of government. If misused, they can compromise the due process rights of individuals and cause immediate financial and reputational harm. The data handling laws of Connecticut primarily address the risks to personal privacy that occur when data is released directly to the public. Few provisions address the implications of interagency disclosures. As Connecticut transforms its system of databases into an integrated data network, its laws must evolve with the technology. Due process provisions need to be central to data matching plans and formal matching pacts need to be drafted to ensure that personal data is only transferred through proper channels.

V. CONCLUSION

The State of Connecticut is leading the country in its plans to integrate its data handling technology. The plan is technically ambitious, but proceeds upon data privacy laws of the past. The state’s current laws primarily address the disclosure of sensitive pieces of data to the public. Connecticut law, however, sparsely addresses interagency transfers of data and the extent to which public information should be made available on-line. As the state rebuilds its information technology system, so must it rethink its data privacy laws.

This paper has put forth a number of suggestions on how to improve Connecticut’s safeguards for personal privacy in the digital age. This paper, for one, advocates that prior to the posting of non-FOIA records on the Internet, strong procedural safeguards need to be enacted to ensure that only valid and necessary data be made available.

Furthermore, non-FOIA disclosures should be restricted to release only data that is essential to publicly endorsed private transactional interests. Connecticut’s Driver’s Privacy Protection

information, along with any copies made therefrom, or makes such returns or return information undisclosable in such manner as the commissioner may prescribe and furnishes a written report to the commissioner identifying the returns or return information that were made undisclosable. See id.
Act, for example, should be reconfigured to limit the disclosure of personal data when the state is merely verifying a third party's information.

Finally, the State of Connecticut should modify its laws regarding interagency data matching plans. Due process protections should be implemented to prevent the government from taking adverse action based on secondhand data. The law, moreover, should require agencies to enter into formalized data sharing agreements, limiting the extent to which personal data can be freely transferred between agencies.