# IDENTIFICATION CARDS WITH DATA ENCODING DEVICES AND THREATS TO PERSONAL PRIVACY: THE NEW BELLEROPHONTIC LETTERS*

Richard Glover**

## I. The Privacy Problems Represented by Encoded Information on Identification Cards

Individuals increasingly rely on identification cards with electronically encoded information. These types of cards, commonly called 'smart cards', are currently capable of containing many kilobytes of information - literally dozens of pages of data or photographs.[1] Although the technology required to place this data onto such a card and to read it is unsophisticated, it is generally not available to the carrier of the card. These cards contain data that is possibly unknown to the cardholder and is circulated by the cardholder. The cardholder lacks control over what can be read or placed on the card, nor is s/he able to verify the accuracy of the data. This lack of control raises concerns about personal privacy regarding the data contained on the

---

* "At that time there arrived at [King Iobates'] court a gallant young warrior, whose name was Bellerophon. He brought letters from Proetus, the son-in-law of Iobates, recommending Bellerophon in the warmest terms as an unconquerable hero, but added at the close a request to his father-in-law to put him to death. The reason was that Proetus was jealous of him, suspecting that his wife Antea looked with too much admiration on the young warrior. From this instance of Bellerophon being unconsciously the bearer of his own death warrant, the expression 'Bellerophontic letters' arose, to describe any species of communication which a person is made the bearer of, containing matter prejudicial to himself." Thomas Bulfinch, *Bulfinch's Mythology: The Age Of Fable Or Stories Of Gods And Heroes* (Nelson Doubleday Books, 1969) at 130.

** The author wishes to thank the following individuals for their assistance in making this article possible: the author's classmates in Privacy Law during the Fall 1995 semester at the Gonzaga School of Law for their continued interest in the development of privacy law which generated much valuable thought provoking discussion; Ms. Suzanne Frishman, Ms. Michele Woodruff, and Mr. Heiko Coppola for assistance in producing a more error-free and coherent article; and Professor Stephen Sepinuck for his invaluable insights into privacy law and his patient tutorage of this author. This article is dedicated to the late Mrs. Norma Jean Glover for her selfless dedication to humanity and her limitless encouragement and support of this author. To paraphrase a famous literary figure, I can only say this of my mother: of all the souls I have met in all my travels, hers was the most human.

[1] DigiCash, bv., DigiCash - Numbers That Are Money (Company Brochure) (1994). Online: <http://www.digicash.com/>.

cards.

The current law provides insufficient protections for this information. The encoded information on advanced 'smart-cards' deserves no less privacy protection than records held in ordinary third party computer databases. The information on the cards can be extensive, representing financial data, history of employment, medical records, or even a record of the holders' presence at a specific location at a specific time. This information could be used by others to deny credit, future employment, medical services, and even civil or criminal due process. The information on the cards is potentially very prejudicial to the cardholder and may remain unknown to the cardholder. There is no specific procedure to follow that will allow the cardholder to decode and verify the information on the card.

There is no means available for the cardholder to place an explanatory statement of personal information on the card. These rights of disclosure, verification, comment, or correction are frequently conferred to individuals in connection with computer records held in databases controlled by third parties. However, due to their nature, the records on the card escape most of these protections.

Most people cannot simply stop using these cards. For instance, in some cases, legal mandates may force individuals to use the card in order to obtain the benefits conferred by the issuing agency. As technology makes data encoding on identification cards easier, cheaper, and faster, individual cardholders lose the ability to protect personal information from unintended disclosure. An example is the Social Security card. Without this card and assigned number, a citizen or authorized alien may not work in the United States.[2] In other cases, individuals may be severely handicapped by not having an accepted form of identification, such as a driver's license or food stamp card. Although there is no law requiring a person to be employed, to rely in a crisis upon food stamps, or to get a driver's license, life without these items is possible only by simple subsistence, a lifestyle increasingly rare in today's technological society.

Computer records in the hands of third parties are difficult enough to control. However, the computer records on identification cards exacerbate these control problems by exploiting the lack of any cohesive policy that consistently applies to computer records, wherever they are located or in whatever form they take. Current statutes are fragmented, and there is no cohesive policy of protection for all

---

[2] 26 C.F.R. § 31.6011(b)-2 (West 1995).

computer records.

> Although there is a substantial number of statutes and regulations that collectively might be called the 'law of personal-data record keeping', they do not add up to a comprehensive and consistent body of law. They reflect no coherent or conceptually unified approach to balancing the interests of society and the organizations that compile and use records against the interests of individuals who are the subjects of the records.[3]

While the common-law recognizes specific causes of action for invasion of privacy, the offending actions must represent unreasonable intrusions in order to be considered tortious. This level of activity is infrequently found. Perhaps, the reason is that most individuals generally accept the existence of computerized records, or society is cynical and feels helplessness in the new age of computerization. Furthermore, for some forms of common law actions to succeed, there must be publicity given to personal information. This is infrequently done. Most data-encoded card issuers will access the data for internal use only, rarely publicizing anything. At most, they may place new information on the card, giving that information only to the owner-cardholder.

The compilation of consumer information by credit card companies is not unusual. At least one court has held there is no invasion of privacy in doing so. The American Express Company categorized its customer/ cardholders by certain criteria obtained from internal computer analysis and sold this information to third party marketing firms. The marketing firms used the information to target the cardholders as potential customers for other products. The court in *Dwyer* v. *American Express Company*[4] concluded that there was no invasion of privacy for an unreasonable intrusion upon the cardholders' seclusion by the company in selling these categorizations of their customers. The court further concluded that the plaintiff did not establish an important element of the tort, an unauthorized intrusion or prying into the plaintiff's seclusion. "By using [the card], a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information

---

[3] U.S. Department of Health, Education and Welfare, *Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (U.S. Department of Health, Education and Welfare, 1973) at 34-35.

[4] *Dwyer* v. *American Express Company*, 652 N.E.2d 1351 (Ill. Ct. App. 1995).

voluntarily given to it and then renting its compilation."[5] This language implies that the publication of an individual's spending habits when compiled by a merchant is permissible, since the individual has voluntarily provided the information.

The holding in *Dwyer* is troubling, since the court refused to recognize a cause of action for disclosure of private information unless the disclosure is sufficiently outrageous as to be highly offensive to a reasonable person. The spending habits of individuals were obtained from computer records and the disclosure was wholly unauthorized by the individual. Spending habits, buying preferences, and consumer patterns are arguably information that is 'just none of anybody else's business'. Disclosure of this information is by definition a privacy violation. The practical extensions of the problem in *Dwyer* are particularly troubling. The disclosure of consumer spending patterns for pecuniary gain may not be a violation of an individual's privacy, but it is arguably more than a minor inconvenience. The likely result of the particular disclosure involved in *Dwyer* is the targeting of the plaintiff for unwanted solicitations. If those solicitations are merely advertisements for other products or services, the individual has a ready answer - the nearest wastebasket. If the solicitations are telephone calls at an inconvenient time or in a disruptive manner, the individual may argue a greater injury, but even this intrusion is hardly a "hanging offence."[6] However, it is probably a matter of time before computer records are routinely analyzed to glean information that will result in much greater injury than the plaintiff complained of in *Dwyer*. Individuals may be unable to prevent injuries by merely getting a larger wastebasket or a screening answering machine. Their only defence to greater injury lies in the protection of the information from improper disclosure to a party able to inflict the damage.

The following situations exemplify some hypothetical privacy problems presented by data encoding devices on identification cards. These situations have the potential to cause much greater harm or injury to the cardholder than the injury the plaintiff suffered in *Dwyer*:

A. Agencies administering food stamp programs can replace paper food stamps with a debit card. Indeed, Texas has adopted the 'Lone Star' card: a computer debit

---

[5] *Ibid.*

[6] See *e.g.* 47 U.S.C. § 227 (1996); 47 C.F.R. § 64.1200 (1996) (conferring a private cause of action, including statutory damages of $500 for each offence against telephone solicitors that act in a harassing manner).

card to replace food stamps.[7] The card could contain a data recording device that makes a record of each purchase, including total amounts of the purchases, a description of each item purchased, and the date, time, and place of each purchase.[8] While this system may enable a reduction in fraud and abuse of welfare programs, it also makes information about a transaction between the individual and the single merchant less secure. Data so encoded on the card would have economic value to subsequent merchants who come into temporary possession of the card. The value of such information is demonstrated by the activities of the defendant in *Dwyer*.[9] The data would be available to any other merchants or marketing agents to whom the cardholder presents the card, since it would be potentially readable by all who possess the card and has access to a proper reading device. A privacy problem arises by the unintentional disclosure of personal and potentially embarrassing information by the cardholder. The information might disclose a pattern of arguably inappropriate purchases.[10] A person requiring public assistance generally lacks a meaningful alternative to accepting public aid subjecting their lives to increased levels of intimate control or scrutiny can have consequences ranging from the mere embarrassing to the devastating. Consider the potential effect on an individual who is sent an advertisement from a merchant that has deduced the individual's preference to buy a particular product from information on a food stamp card. Such an advertisement could be a mere annoyance, much like the situation in *Dwyer*. However, consider the effect should the advertisement be discount coupons for the individual's favourite brand of over-the counter contraceptives, and they are received by the individual's sterile spouse.

B. State driver's licenses are currently being issued containing data encoding

---

[7] "Texas no longer uses paper food stamp coupons. The state now uses an electronic debit card – the Lone Star Card. After making your purchases, you scan the Lone Star Card through the same machine that accepts bank and credit cards." Texas Dept. Human Services, online:<http://www.dhs.state.tx.us/programs/texasworks/foodstampfaq.html>.

[8] The Texas card does not appear to currently contain such capabilities, but enabling such capabilities to the current system is nearly a trivial administrative software change.

[9] *Dwyer*, *supra* note 6.

[10] Defining an 'inappropriate purchase' is beyond the scope of this discussion. Arguably, purchases of expensive luxuries, such as prime fresh seafood, imported vegetables during off growing seasons or fertility prediction devices to facilitate a planned pregnancy are inappropriate by those on public assistance. However, the intimate control of individuals' personal lives is problematic in a society that portends to value freedom of choices and personal liberties, particularly when those individuals do not subject themselves to such control voluntarily.

devices, either as magnetic stripes or data chips.[11] The data recording devices are not readable without special equipment, thereby depriving the holder of knowing what data is contained on this most used identification card. The card could hold a record of each time it discloses the identifying encoded information. A driver's license is a commonly accepted form of identification. It is becoming increasingly common as the only acceptable form of identification. To cash a check for example, many merchants demand a current driver's license. With unsophisticated computer systems, a system could easily be implemented to identify the cardholder that records information on the card about each time the card is used. Such information is invaluable to law enforcement because it provides a record of a suspect's location and travels. The information would also have value in discerning a consumer's buying patterns and habits. Once again, a privacy problem arises by the unintentional disclosure of information by the cardholder.

C. Employment records might also be encoded on Social Security cards. Social Security numbers and cards are becoming increasingly common as means of identification.[12] The Social Security Administration continues to be plagued by fraud arising from easily counterfeited Social Security cards. Congress has proposed the adoption of identification cards containing electronically encoded data.[13] As the enhanced Social Security Card becomes evidence of authorization to accept employment, information such as past income levels and retirement savings becomes available to potential employers.[14] Not only is there a privacy problem in unintentional disclosure of information by the cardholder, but the possession of this information by a potential employer is arguably inappropriate. Even if the information is true, the potential employer may refuse employment to the applicant

---

[11] The author has examined examples of driver's licenses from several states, including Oregon, Texas and Arizona, that contain magnetically sensitive media capable of electronic data storage. See also H.R. 2150, 54th Leg., Reg. Sess. 12 (Wash. 1996) (funding a study of methods to increase the reliability of identification cards through the use of "biometric systems.").

[12] The author is well acquainted with the exception authorising a demand by educational institutions for presentation of the card to receive federally insured student loans. See 34 C.F.R. § 682.201 (West 1995).

[13] "The Secretary [of Health and Human Services] shall cause to be issued enhanced Social Security account number cards to United States citizens.... The cards...shall...be uniform in appearance,...be as tamper-proof and counterfeit-resistant as is practicable,...contain a photograph and such other identifying information that is specific to each person as the Secretary shall determine... contain the name, sex, date of birth, citizenship status, and Social Security account number of the issue, and...incorporate a machine-readable encoding of the information contained in the card." H.R. 1018, 104th Cong., 1st Sess. 301(d) (1995).

[14] Contributions to an income reduction plan (a '401k' retirement savings account) are deducible by comparing gross income to income reported for FICA taxation. Author's personal experience.

claiming that his current retirement savings is subjectively too low, an indication of fiscal irresponsibility. It is arguable that it is acceptable for an employer to make discretionary business decisions based on this information. However, the employer may be denying employment to an individual who desperately needs that income. The individual may have a perfectly valid reason for having low retirement savings. Yet, the individual may be denied the opportunity to explain[15] since this explanation could not be encoded on the card or disclosed to an employer anxious to fill a highly competitive position. If the encoded information is erroneous, the applicant probably will never know why employment offers are never forthcoming.

Each of these situations contains common elements: individuals identifying themselves by presenting a computer compatible card; each basic type of card (without the enhanced data gathering devices that are easily manufactured and distributed) are currently widely in use; the information contained on the cards has value to others; the information is potentially true; and, the individual carrying the card cannot readily know what information is on the card, verify the correctness of the data, or comment on the meaning of the data.

While disclosure of the information contained on the card has the potential to be very embarrassing to the cardholder, that fact alone does not cause the greatest concern. The disclosure of information in an uncontrolled manner, without the knowledge and explicit consent of the cardholder, and without the ability to verify the information, has the potential to deny credit, employment, and civil or criminal due process. Even accurate information disclosed without sufficient explanation can be harmful to the individual. If the information is incomplete, it can reflect badly on the individual. Clearly, if the information is erroneous, there is greater potential for harm. The disclosure of information through the use of encoded identification cards, therefore, is more than a classic privacy problem where the dissemination of accurate information may be embarrassing or may become the subject of gossip or harassment.

These devices represent advancements that can provide substantial benefits to our society, but the benefits come at a cost to personal privacy. The driver's license

---

[15] For a humorous example of the Social Security Administration's record of placing conflicting information on Social Security Cards, refer to the written instructions on the back of currently issued cards. The author's card reads, "This card belongs to the Social Security Administration and you must return it if we ask for it. If you find a card that isn't yours, please return it to: [the SSA's government office address]." Literal compliance with these instructions is patently absurd, as they require all cards to be returned.

enhancements could be an effective law enforcement tool and the changes to the food stamp program and social security cards might reduce fraud and counterfeiting problems that result in waste and abuse. However, the data encoded on the cards requires special (although unsophisticated) equipment for access, and individuals will generally not have access to this equipment. Without such means, the cardholder lacks the means to verify the correctness or extent of the data encoded. Without knowledge of the information the card contains, the individual has a limited means to explain or comment on the data. The ability to comment is a common right statutorily conferred in similar contexts.[16] The right is designed to protect individuals against overreaching by third party possessors of an individual's personal information.

We may become our own worst enemies in destroying our privacy in the age of increasing computerized information encoding. We spread the virus of undesirable, incorrect, incomplete, misleading or damaging information without our knowledge. By merely identifying ourselves, we could convey unverified and potentially damaging information to others. Interactions are so numerous and routine that we have become apathetic about monitoring what we disclose.[17] Society needs controls on private information about individuals to prevent abuse by holders of that information. On one hand, we want others to know some things about us, our credit worthiness for example, so we may negotiate goods or services on advantageous terms. However, the right of privacy is based on the need for individuals to control the amount of their interaction with the rest of society.[18] An identification card can

---

[16] See *e.g. The Privacy Act of 1974*, 5 U.S.C. § 552a(d) (1995) (conferring a right to individuals to comment on the accuracy of government held records).

[17] "In this information-intensive society, dependent upon the marvels of the modern computer, we frequently exhibit indifference toward intrusions into our personal privacy. Confronted with ever-advancing technological developments, we have resigned ourselves to the inevitability of our private affairs appearing on silicon microchips in computers too numerous to count. The majority's opinion reflects this societal apathy...." *Peninsula Counselling Center* v. *Rahm*, 105 Wash. 2d 929, 937 (1986) (Pearson J., dissenting).

[18] Alan Westin defined privacy as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Alan Westin, Privacy And Freedom 7 (1967). Hyman Gross defined privacy as "control over acquaintance with one's personal affairs." Hyman Gross, Privacy and Autonomy, in NOMOS XIII: PRIVACY (1971). "The condition of human life in which acquaintance with a person or with affairs of his life which are personal to him is limited." Hyman Gross, "The Concept of Privacy" 42 N.Y.U. L. Rev. 34, 36 (1967) (emphasis omitted). "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." Samuel Warren & Louis Brandeis, "The Right to Privacy" 4 Harv. L. Rev. 193, 198 (1890).

contain massive amounts of information unavailable to the holder and possibly irrelevant to a particular transaction. When a cardholder offers the information to others unknowingly by presenting his card, there may be an implicit authorisation to transfer the information contained on the card. However, for most transactions, the cardholder is not necessarily intending authorization to transfer all the information on the card, only that which is necessary to the transaction.

We can reap the potential benefits of reduced fraud and increased efficiency that these identification cards provide if there are sufficient safeguards to control and verify the data spread through their use. The real threat comes from the individual's inability to obtain the benefits of the program for which the cards were intended without unintentionally disclosing inaccurate, incomplete or irrelevant personal information. Once proper safeguards are in place, individuals can be assured of the security of the information on the cards. Without proper safeguards, personal interests will yield to commercial interests in extracting value from information gathered or provided by the individual. These personal interests are important rights in maintaining seclusion, in creating the ability to intentionally interact in an informed and controlled manner, or in simply "being let alone." Statutory requirements or common-law principles would put those who would interfere with these rights on notice regarding appropriate ways to utilize this information. This is a proactive deterrent. It discourages secret, erroneous, or incomplete dossiers that invade privacy interests.[19]

The current law is unable to provide suitable safeguards for inappropriate disclosures. Therefore, new procedures are essential. It would be appropriate to require personal information encoded on a card to be disclosed to the cardholder upon demand. Cardholders must be afforded an opportunity to have the information corrected by the encoding entity upon proof that the data is incorrect or to comment on the meaning of the data. If the latter applies, the comments must always be

[19] Secret dossiers and files can do more than threaten harm. "Previous dictatorships have repressed society with machine guns, tanks, and armies, but repression may come in the form of an Orwellian psychology, with data banks and dossiers." Toby Solomon, "Personal Privacy and the '1984' Syndrome" 7 W. New Eng. L. Rev. 753, 760 (1985). "[T]yrannies thrive by granting great secrecy to government but very little to individuals, while democracies thrive by opening government to public scrutiny and closing citizens' lives to governmental prying." Judge Bazelon, "Probing Privacy" 12 Gonz. L. Rev. 587, 592 (1977). It seems the ultimate irony to deposit the secret records on the individuals themselves and then allow them to be the destroyers of their freedoms.

transmitted at the same time the related information is disclosed.[20] As a matter of common law, courts should recognize a cause of action that protects the private interests individuals have in the data encoded upon these cards. As a general presumption, information encoded on the card should be considered private. Any electronic transmission of information from an identification card to others without express (not merely implied) authorization should be tortious.[21] Only by eliminating the proliferation of the data can an individual be given any control over its release, since once the 'cat is out of the bag,' there is no controlling where that cat may wander. Recognition of a cause of action would provide an important deterrent protecting individuals' interests.

## II. Existing Statutes Do Not Adequately Protect Individuals' Privacy

Personal information is protected by five federal statutes: The Privacy Act of 1974,[22] the Electronic Communications Acts,[23] the Driver's Privacy Protection Act,[24] the Right to Financial Privacy Act,[25] and the Fair Credit Reporting Act.[26] Each Act protects certain specific types of records and prohibits certain disclosures. Taken together, the statutes seem to provide for a policy of protecting private information in the hands of third parties.

None of the federal statutes designed to protect privacy adequately deal with the problems associated with encoded identification cards. Because of the cardholder's role - unwitting as it may be - in the release of information contained on an encoded identification card, the release apparently does not qualify as the type of "disclosure" or "interception" of information prohibited by any of the five relevant federal acts.

---

[20] These statutory protections are afforded by the *Privacy Act of 1974*, 5 U.S.C. § 552a (1995) to certain governmentally held records, but many critical records, including most card based records, escape such protection.

[21] Improper uses of information for internal use are objectionable as well. However, by restricting information from even coming into the hands of an entity contemplating improper uses, the card loses its function as a data conduit and the potential for improper use is eliminated.

[22] *Supra* note 16.

[23] 18 U.S.C. § 2701-2711 (1995).

[24] 18 U.S.C. § 2721-2725 (1995) (effective July 7, 1995).

[25] 12 U.S.C. § 3401-3422 (1995).

[26] 12 U.S.C. § 3401-3422 (1995).

*The Privacy Act of 1974 does not prohibit data transfers with identification cards*

Identification card data collection and reporting escape the prohibitions of certain information transfers of the Privacy Act of 1974[27] for at least two reasons. First, the Act is intended to restrict information dissemination by the government,[28] and the Act textually protects only transfers or collections of information by government agencies.[29] Second, the Act provides protections only to certain types of records: those "contained in a system of records."[30] The scope of the protections conferred is quite limited and likely does not properly protect private information.[31] The Act requires governmental action to trigger the protection of the Act.[32] The government entity may put in place the technological means to have the card collect and encode information upon presentation by the cardholder. The government agency therefore is not a holder of the record, nor does it actively collect any data. It is the individual

---

[27] 5 U.S.C. § 552 (1995).

[28] 5 U.S.C. § 552a (1995).

[29] From the legislative history of the act: "The purpose of [the Privacy Act] is to promote *governmental respect* for the privacy of citizens by requiring all departments and agencies of the executive branch and their employees to observe certain constitutional rules in the computerisation, collection, management, use, and disclosure of personal information about individuals. It is to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the *Federal Government* and with respect to all of its other manual or mechanised files. It is designed to prevent the kind of illegal, unwise, over broad, investigation and record surveillance of law-abiding citizens produced in recent years from actions of some over-zealous investigators, and the curiosity of some government administrators, or the wrongful disclosure and use, in some cases, of personal files held by *federal agencies*. It is to prevent the secret gathering of information on people or the creation of secret information systems or data banks on Americans by employees of the *departments and agencies of the executive branch*. It is designed to set in motion for long-overdue evaluation of the needs of the *Federal Government* to acquire and retain personal information on Americans, by requiring stricter review within agencies of criteria for collection and retention. It is also to promote observance of valued principles of fairness and individual privacy by those who develop, operate, and administer other major institutional and organizational data banks of government and society." S. Rep. No. 1183, 93rd Cong., 2nd Sess. 1974, 1974 U.S.C.C.A.N. 6916 (Leg.Hist.) [italics added].

[30] "No *agency* [as defined in 5 U.S.C. § 552(a) (1995)] shall disclose any record contained in a system of records... except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains...." 5 U.S.C. § 552a(b) (1995) [italics added].

[31] Interestingly, the term "individual" is defined by the Act: "[T]he term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence." 5 U.S.C. § 552a(a)(2) (1995). Visitors to this country apparently are not protected from government record keeping the same as citizens or lawful aliens.

[32] See *supra* note 16.

cardholder who is repeatedly collecting and disclosing the information by presenting the card for identification.

The records on the card are not contained in a protected "system of records."[33] The governmental agency has no control over the records on an identification card: the individual cardholder determines where and when the card is presented to others. The agency cannot verify the accuracy of any of the information encoded on an identification card.[34] Indeed, until the card is presented to the agency (an uncertain event), the government has no means of even knowing of the existence of any records on the card. Therefore, the encoded data on the card is not a government record and thereby escapes the protection of the Act.

The Act prohibits "disclosure,"[35] but does not define the term. Encoding data on the card may not be a disclosure. Providing a system of records that is not secure against outside intrusion may not by itself constitute disclosure.[36] Protection of the records only applies when there is a disclosure of the records in the files themselves.[37] Where the records are only indicative of an interaction with a government agency, the records are not protected from disclosure.[38]

Greater protections than those afforded by the Privacy Act are needed. Disclosure of records protected by the Privacy Act receives special treatment. The

---

[33] "[T]he term 'record' means any item, collection, or grouping of information about an individual that is *maintained by an agency*, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4) (1995) [italics added]. "[T]he term 'system of records' means a group of any records *under the control of any agency* from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5) (1995) [italics added].

[34] When the agency uses the records for its own internal purposes, the records must be reasonably accurate, but no such obligation arises when the agency transfers the records to other agencies. *Doe* v. *United States Civil Service Comm'n*, 483 F. Supp. 539 (S.D.N.Y. 1980); *R.R.* v. *Dept. of Army*, 482 F. Supp. 770 (D.D.C. 1980); *Perry* v. *F.B.I.*, 759 F.2d 1271 (7th Cir. 1985), reh'g granted, 781 F.2d 1294 (7th Cir. 1986), cert. denied, 479 U.S. 814 (1986).

[35] 5 U.S.C. § 552a(a)(5) (1995).

[36] *King* v. *Califano*, 471 F. Supp. 180 (D.C. Cir. 1979) holding that data that was previously known publicly could not be the source of a disclosure violating the Privacy Act.

[37] *Krowitz* v. *Department of Agriculture, U.S. Forest Service*, 641 F. Supp. 1536 (W.D. Mich. 1986), aff'd, 826 F.2d 1063 (6th Cir. 1987), cert. denied, 484 U.S. 1009 (1988).

[38] *Tobey* v. *N.L.R.B.*, 40 F.3d 469 (D.C. Cir.1994).

Act requires disclosure of the records to the individual to whom the record pertains upon demand by that individual;[39] and, for an amendment of the record, upon proof of error in the record.[40] Most importantly, the Act contains a comment procedure allowing the individual to place an explanatory statement into the file.[41] An agency that maintains a system of records has specific duties with respect to them under section (e) of the Act.[42] These twelve separate sections represent excellent safeguards for personal information.

The Act's effectiveness in protecting information on identification cards is otherwise limited. The Act provides for remedies against only the agency and provides no deterrent to a private entity seeking to profit from the data on the cards.[43] Card based records can be neither governmental nor systematic, so there are no protections afforded by the Act.

*The Electronic Communications Acts do not protect card based records*

Cardholders may look to Electronic Communications Acts[44] (E.C.A.s) for a remedy against those who monitor their actions electronically. In essence, monitoring occurs when a private entity records information in a non-secure manner on a consumer's identification card: the encoder-merchant is communicating information to another. Congress expanded the E.C.A.s, originally directed at securing oral communications, to provide protections for "electronic communications" that are "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo optical system."[45] Protections are provided for "electronic communications systems" defined as "any wire, radio, electromagnetic, photo optical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related

---

[39] 5 U.S.C. § 552a(d)(1) (1995).

[40] 5 U.S.C. § 552a(d)(2) (1995).

[41] See 5 U.S.C. § 552a(d) (1995) conferring a right to individuals to comment on the accuracy of government held records.

[42] Reproduced in Appendix.

[43] 5 U.S.C. § 552a (g),(i) (1995).

[44] Title III of the *Crime Control and Safe Streets Act of 1986*, the *Electronic Communications Acts of 1986 and 1993*.

[45] 15 U.S.C. § 2510(12) (1995).

electronic equipment for the storage of such communications."[46] Data recording devices in identification cards may arguably fall under this category since the chips or magnetic media in the cards are capable of transmitting recorded messages.

The protections afforded by the E.C.A.s do not clearly attach to protect records encoded on cards. Interception of communications is not prohibited when one of the parties to the communication has consented to the interception.[47] A third party reading data encoded information on the identification card by another reader-user of the card would be such an interception, but arguably, the relinquishing of the card to the third party manifests the necessary consent to such action.

*Information encoded on a Driver's License will not be protected by The Driver's Privacy Protection Act*

Data encoded on a state driver's license is potentially protected by The Driver's Privacy Protection Act.[48] However, these protections are very narrow. The Act only protects information from disclosure by the government and their agents. Most importantly, protections are afforded only if disclosed "knowingly." It is doubtful that a record that was placed on the license by an independent third party could be thought of as knowingly disclosing by the agency.[49] The first presentation of the card containing the records is arguably disclosure by the cardholder, not the agency. The Act provides for fourteen specific exceptions. Many are directed at allowing disclosure for legitimate law enforcement purposes. A broad exception is made allowing disclosure:

(3) For use in the normal course of business by a legitimate business or its agents,

---

[46] 15 U.S.C. § 2510(14) (1995).

[47] 15 U.S.C. § 2511(2)(c),(d) (1995).

[48] 18 U.S.C. § 2721-2725 (1995) (effective July 7, 1995). The Act protects "personal information," which is defined in the Act as "information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status." 18 U.S.C. § 2725(3) (1995). Disclosure by "a State department of motor vehicles, and any officer, employee, or contractor, thereof..." is prohibited. 18 U.S.C. § 2721(a) (1995).

[49] For example, driver's licenses with internal microprocessors could be programmed to record the time and location of each point where the card is accessed for identification information. The agency will be without knowledge of any of this data because the circulation of the card is at the discretion of the cardholder. Without safeguards on this data, all future holders of the card potentially have access to this record.

> employees, or contractors, but only
>
> (A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and
>
> (B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.[50]

This exception seems to imply that any "legitimate" business can demand verification of a customer's medical or disability status should it be encoded on a state driver's license.[51] If such information is encoded on the identification card and the holder offers the card to a business, a business is entitled to verify the personal information submitted by the cardholder, though that information is not conveyed for that reason.[52] Textually, an employer could require employees to submit their driver's licenses for inspection to verify their eligibility for insurance. Indeed, there is a specific exception allowing for this very purpose.[53] However, there are no provisions in the Act to provide for verification of the encoded data by the cardholder. Should the information be erroneous or misleading, the individual could suffer a loss or denial of employment as a consequence of an erroneous assumption.

There is a need to protect certain driving records from random disclosure. The term "personal information" specifically excludes "information on vehicular accidents, driving violations, and driver's status."[54] Such information could be encoded on a driver's license in an effort to speed up the processing of traffic stops without violating the Act. This information could be highly prejudicial in an

---

[50] 18 U.S.C. § 2721(b)(3) (1995).

[51] The need for use of special driving equipment, such as additional mirrors, automatic transmissions, or corrective lenses is frequently noted on current licenses where appropriate.

[52] Some licenses are limited to daytime only privileges, usually indicating a night vision deficiency. The value of recognizing an employer's right to deny such an individual employment because the employer subjectively fears an accident "if the lights ever go out" is dubious at best.

[53] Disclosure is permitted "[f]or use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting." 18 U.S.C. § 2721(b)(6) (1995).

[54] 18 U.S.C. § 2725(3) (1995).

employment context.[55] The danger is not that accurate information would be disclosed. The danger lies in the possibility that accurate information may be taken out of context with no opportunity for the cardholder to explain or respond. Moreover, if the information on the card is inaccurate, by clerical error or otherwise, the cardholder may never know of the error. Meanwhile, the prospective employer has assumed the applicant to be a liar. The cardholder must have the means to know exactly what information is disclosed and under what circumstances. Without a procedure to make records that are available for public inspection verifiable, accountable, and correctable, individuals face the possibility that erroneous decisions will be made about them. These decisions have the potential cause them great harm.

There are other remedies for wrongful denial or termination of employment.[56] These remedies generally reward retroactive damages to a wronged person from an entity acting tortiously. A person faced with the 'cat out of the bag' release of information faces the practical problem of perhaps never knowing what is preventing the offers of employment. Even if the reason is eventually disclosed, an unemployed individual may be unable to afford to pursue legal remedies. The best protection for cardholders is proactive prevention of improper disclosure.

*The Right to Financial Privacy Act prohibits disclosures only to governmental agencies and does not control actions of private entities*

Financial information can be encoded on an identification card. The 104th Congress considered implementation of an enhanced Social Security Card.[57] Enhanced Social Security Cards have the potential to contain significant amounts of financial information about the cardholder, so there is a need to protect this personal information. The Social Security Administration discourages use of the card as identification, but acknowledges increasing use of social security numbers for record keeping by the private sector and various governmental agencies.[58] No law

---

[55] It is highly likely an employer will be reluctant to hire someone with a history of arrests for drunk driving (even if not convicted) considering the increased medical insurance risk such a person might represent. It is arguable that employers have a legitimate interest in protecting their business from financial losses. Few would argue that it is fair to allow employers to have an absolute right to do so at the expense of great harm to applicants based on incorrect or misleading information.

[56] For example, see *Civil Rights Act of 1964*, 42 U.S.C. § 2000e-2000e-17 (1995); *Fair Labor Standards Act of 1938*, 29 U.S.C. § 206(d), 216, 217 (1995).

[57] H.R. 1018, 104th Cong., 1st Sess., 301(d) (1995).

[58] Department of Health and Human Services, Social Security Administration, SSA Publication No. 05-10002, online: <http://www.ssa.gov/pubs/10002.html>.

generally restricts the use of social security numbers by the private sector.[59] Employers as well as state agencies can require the individual to display the card.[60] Educational institutions can demand that the cardholder present the card before disbursing federally insured student loans.[61] Any financial information on the card is potentially offered up for inspection each time an enhanced card is presented. There are no technical reasons why the possessor of the card would be unable to encode additional information on the card, or download information that is already on the card.

There is a legitimate purpose for encoding financial information on the card: the Social Security Administration is charged with monitoring individuals' eligibility for benefits under the Social Security Act. Any efficient means of collecting data to determine an individual's eligibility is in accordance with this Congressional mandate. ¡The current complex arrangement of exchanging forms quarterly between employers and the I.R.S.[62] could be considerably enhanced with a system that allows employers to encode an employee's card periodically. The cardholder could then present the card to Social Security Administration for verification when applying for benefits. The card itself could be programmed to be a source of benefits by doubling as a debit card. This would allow an individual immediate access to his benefits and reduce the reliance on paper forms and records.

The holder could look for protections in the Right to Financial Privacy Act,[63] but there are insufficient protections[64] conferred by that statute. The basic protection afforded by the Act is that "[n]o financial institution, or officer, or agent of a financial institution, may provide to any Government authority access to or copies of, or the information contained in, the financial records of any customer except in

---

[59] *Ibid.* See also U.S. Department of Health, Education & Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (U.S. Department of Health, Education & Welfare, 1973) at Ch. VII, VIII, discussing the history and use of the SSN as a general uniform identifier, and recommending restrictions on its use.

[60] 42 U.S.C. § 1320b-7 (1995); see also 45 C.F.R. § 205.52 (1995).

[61] 34 C.F.R. § 682.201 (1995).

[62] The Internal Revenue Service collects Social Security Taxes for the Department of Health and Social Services. 26 U.S.C. § 3102 (1995).

[63] 12 U.S.C. § 3401-3422 (1995).

[64] Although the protections are narrow, civil penalties, including punitive damages, are authorized under the statute. 12 U.S.C. § 3417 (1995).

accordance with the provisions of this chapter."[65] The key terms of this protection are defined by the Act, but the protections afforded by this statement are only afforded to prohibit disclosure to government agencies. This Act does not provide for sufficient protection against disclosure to private entities of the highly personal information that could be contained on such an enhanced card.

The text of the Act further narrows the protections, even though the Act defines "financial institution" broadly.[66] The "financial records" protected by the Act are very specific: "an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution."[67] The Act prohibits disclosure only to an agency of the federal government: state entities are immune from controls of the Act.[68] Additionally, one must become a "customer" of an institution before these protections attach.[69] Therefore, this Act provides only for relief from intrusions by the federal government into records that relate specifically to transactions with the financial institution that created them. Disclosure of financial records to an employer or potential employer would not be prevented by the Act (unless that employer is the federal government).

Protection of these records is important. It seems hardly fair to allow a potential employer free access to all previous employment and financial records of an applicant without giving the applicant the opportunity to verify the accuracy of the records or explain the circumstances underlying certain facts in the records. For purely personal reasons, an individual may not wish to disclose the name of a previous employer without the ability to fairly explain the nature of the past employment relationship. The individual may fear an unfavourable recommendation that could be easily explained, given the chance. Past involvement in a particular job,

---

[65] 12 U.S.C. § 3402 (1995).

[66] "[A]ny office of a bank, savings bank, card issuer as defined in section 1602(n) of title 15, industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands." 12 U.S.C. § 3401(1) (1995).

[67] 12 U.S.C. § 3401(2) (1995).

[68] "'Government authority' means any agency or department of the United States, or any officer, employee, or agent thereof." 12. U.S.C. § 3401(3) (1995).

[69] "'[C]ustomer' means any person or authorized representative of that person who utilized or is utilizing any service of a financial institution, or for whom a financial institution is acting or has acted as a fiduciary, in relation to an account maintained in the person's name." 12. U.S.C. § 3401(5) (1995).

without an opportunity for explanation, could be highly prejudicial. Few, for example, would argue that an employer that pays for an employee health care policy for its employees would be reluctant to hire an ex-employee from a toxic waste site. An individual may not wish to disclose his/her salary history. The individual may fear that the employer may not offer employment at a reduced salary because the individual will continue to look for higher paying jobs while accepting a temporary position. The records may also show a period of non-employment. If, for example, non-employment was due to medical reasons, those reasons might be too personal to disclose. The information becomes prejudicial to the individual seeking employment. However, control, to the extent that the faceless record portrays the individual in a false light, is beyond the individual. This loss of control is contrary to the concept of personal privacy.

*The Fair Credit Reporting Act protects privacy of "consumer reports," but it is unlikely that data encoded on information cards represent a "consumer report" within the meaning of the Act*

The Fair Credit Reporting Act provides individuals with certain statutory protections of privacy of records.[70] The protections extend to "consumer reports," which are defined broadly by the Act.[71] Privacy protections are conferred to "any...other communication," which may possibly include dissemination by consumer data cards. The Act provides protections from disclosure by a broad range of entities.[72] The combination of these definitions covers much ground: a personal characteristic transmitted by "any means" by "any person" is covered by the provisions of the Act.[73]

---

[70] 15 U.S.C. § 1681-1681t (1995).

[71] "[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for – (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) other purposes authorized under [15 U.S.C. §] 1681b...." 15 U.S.C. § 1681a(d)(1) (1995).

[72] A covered entity is defined as "*any person* which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses *any means* or facility of interstate commerce for the purpose of preparing or furnishing consumer reports." 15 U.S.C. § 1681a(f) (1995) [italics added].

[73] *Ibid.*

The nature of the records encoded on an identification card and the means by which they are encoded on the card removes the likelihood that they will be protected by the Act. The Act's protection against disclosure does not attach until the data is collected for dissemination "by" a consumer-reporting agency.[74] There is a specific exemption from the protections provided by the Act for records of transactions between the cardholder and the person making the report.[75] The information that will likely be encoded on the card is information regarding the transaction between a merchant or employer and the cardholder. That data is not protected by the provisions of the Act as long as the merchant or employer does not publish it.[76] Data collected on the card is not protected by the provisions of the Act that allow for corrections of inaccuracies since it is not disclosed to others by a credit reporting agency.[77] For example, if a merchant encodes a record that an individual used his driver's license as identification at a particular time at a particular place, that data escapes protection under the Act.[78] The only person that the merchant gave the information to was the cardholder when the identification card was returned after the transaction. It is the cardholder who then passes the information to the next merchant the next time the card is presented for identification.

The Act fails to provide sufficient safeguards to protect employment and financial records that might be encoded on an enhanced Social Security Card. When applying for employment, the cardholder presents the Social Security Card to verify his/her authorization to work. An employer could use his/her history of unemployment to conclude that the cardholder-applicant has a large consumer debt.

---

[74] 15 U.S.C. § 1681b (1995).

[75] "The term 'consumer report'... does not include (A) any (i) report containing information solely as to transactions or experiences between the consumer and the person making the report; (B) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device; (C) any report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made and such person makes the disclosures to the consumer required under section 1681m of this title." 15 U.S.C. § 1681a(d)(2) (1995).

[76] Similar activity not involving the use of data encoded direct onto a credit card, but compiling summaries of spending preferences that were subsequently sold to third parties from data collected into an external computer database was held to be permissible by the Court in *Dwyer*. See *supra* note 4.

[77] 15 U.S.C. § 1681i (1995).

[78] Such a system has value to check guarantee services in an effort to cooperate with official enforcement against bad check writers. Presumably, an incentive is given to the merchant by the guarantee service, or alternatively, the system is implemented by statute.

The employer may fear the applicant's ability to be trusted with valuable company assets. Similarly, the prospective employer could use records encoded on the card to conclude that the applicant is uninsurable due to a history of working in dangerous industries.[79] Since the courts construe the term "employment purposes" broadly, it is possible that the Act precludes the use of records on the card to deny employment.[80] Indeed, there need not be an actual offer of employment to trigger the protections against gathering data in an employment setting.[81] However, information must satisfy three conditions to constitute a consumer report within the meaning of the Act and be subject to the protections afforded by the Act:[82]

a. The report must be made by a consumer-reporting agency;

b. The information must bear on the consumer's credit status or general reputation; and

c. The information must be used or is expected to be used in a determination of the consumer's eligibility for credit, employment, insurance or other commercial benefit.

The Act fails to protect data encoded on an enhanced Social Security Card because the prospective employer is not a consumer-reporting agency.[83] Until the employer

---

[79] Again, it is arguable that employers have a legitimate interest in protecting their business from financial losses. Few would argue that it is fair to allow employers to have an absolute right to do so at the expense of causing great harm to employees based on incorrect or misleading information.

[80] "[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for- (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) *employment purposes*; or (C) other purposes authorized under [15 U.S.C. §] 1681b ...." 15 U.S.C. § 1681a(d)(1) (1995) [italics added].

[81] *Hoke* v. *Retail Credit Corp.*, 521 F.2d 1079 (4th Cir. 1975), cert. denied, 423 U.S. 1087 (1976).

[82] *Porter* v. *Talbot Perkins Children's Services*, 355 F.Supp. 174 (S.D.N.Y. 1973).

[83] Other cases tell us what is not such an agency. A common exception is the situation where the information supplied is only experiences between the supplier of information and the consumer. *Nuttleman* v. *Vossberg*, 585 F. Supp. 133 (D. Neb.1984) Mortgage companies are usually in this situation: their compilations are usually only for internal evaluations of a customer's creditworthiness. *Oldroyd* v. *Associate Consumer Discount Co.*, 863 F. Supp. 237 (E.D. Pa.1994). Retail department stores extending credit are excluded under the same theory. *DiGianni* v. *Stern's*, 26 F.3d 346 (2nd Cir. 1994) Even when the store supplies information about its own experience to a credit reporting agency, that store does not become a credit reporting agency itself. *Rush* v. *Macy's New York, Inc.*, 775 F.2d 1554 (11th Cir. 1985). Supplying polygraph results is not a consumer report. *Peller* v. *Retail Credit Co.*, 359 F. Supp. 1235 (D.C. Ga.1973), aff'd 505 F.2d 733 (5th Cir. 1974). Employers can use credit information

is established as a consumer-reporting agency, as the term is used by the Act, no liability attaches to the employer's actions. Only consumer reports are protected by the Act and a record is only a consumer report if it is compiled for dissemination specifically dealing with a cardholder's credit worthiness,[84] independent of what the information actually represents.[85] Since part of this test will generally not be satisfied in the context of application for employment, there will be no protection of encoded data on an enhanced Social Security card under this Act.

Cardholders need greater protection of private data encoded on identification cards to prevent employers from reaching faulty conclusions. The denial of employment based on incorrect, misleading, or inaccurate data has the potential to devastate individuals' lives. The Act was intended to prevent abuse by holders of sensitive personal information, but it does not protect data spread through the circulation of identification cards. These types of devastating effects caused by the release of information concerned Warren and Brandeis. They wrote fearing "invasions upon his privacy, subject[ing] him to mental pain and distress, far greater than could be inflicted by mere bodily injury."[86] Without proper protection and without the means for the individual concerned to verify information, prospective employers have tremendous power to cause destruction in the lives of individuals resulting from the improper use of information encoded on social security cards.

*States have not acted to confer statutory protections of card based data*

There has been no rush by state legislatures to solve unintended data disclosure problems. Fifteen years have passed since the drafting of the Uniform Informational Practices Code. Only one state, Hawaii has adopted it.[87] The Uniform Act provides an excellent framework for establishing privacy rights. It even has an optional provision for establishing an agency to oversee the proper balancing of private

---

about employees, and not fear being subject to the provisions of the Act as credit reporting agencies because of their actions: they can even use credit information to discharge an employee. *Wiggins* v. *District Cablevision, Inc.*, 853 F. Supp. 484 (D.D.C.1994). Even the local 'repo man' is not a credit reporting agency when doing nothing more than collecting debts. *Mitchell* v. *Surety Acceptance Corp.*, 838 F. Supp. 497 (D.Colo.1993).

[84] *Henry v. Forbes*, 433 F. Supp. 5 (D. Minn.1976).

[85] *St. Paul Guardian Ins. Co.* v. *Johnson*, 884 F.2d 881 (5th Cir. 1989).

[86] Samuel Warren & Louis Brandeis, "The Right to Privacy" 4 Harv. L. Rev. 193, 195 (1890).

[87] Haw. Rev. Stat. § 92F-1 - 92F-42 (1989).

interests against the need for public disclosures.[88]

When states have acted, it appears that they have done so only in restricting the powers of governmental agencies.[89] There is no authority indicating any trend by the states to enact specific legislation to control or confer rights to informational privacy or otherwise restrict probing by non-governmental entities. The only discernible trend is that state legislatures have been proactive about privacy issues involving personal decision-making and search and seizure but not the dramatic effects of invasion of informational privacy. State legislatures appear to feel political pressures from the likes of Dr. Kevorkian,[90] the Quinlan family,[91] and Oregon Public sentiment.[92] In short, the States have legislative power sufficient to confer additional rights of privacy, but the issue apparently has not yet risen to a level where legislators feel compelled to act. An aggrieved individual may attempt to find relief in a state consumer protection act, but likely will be unsuccessful. These acts generally provide for damages only upon a showing of deceptive or fraudulent acts.[93] There is no viable claim under these types of acts since, in most instances, the information is being downloaded or accessed with the implied permission of the cardholder and no fraud on the part of the accessor is involved.

---

[88] See also Dale F. Rubin, "State Government Records and Individual Privacy: Theoretical and Comparative Approaches" 26 Urb. Law. 589 (advocating the establishment of data protection agencies at a state level).

[89] Eight States, California, Alaska, Montana, Hawaii, Florida, Illinois, South Carolina, and Louisiana have dealt with the issue of privacy directly with changes to their state constitutions. The original constitutions of Washington and Arizona have direct provisions conferring rights of privacy. K. Gormley & R. Hartman, "Emerging Issues In State Constitutional Law" 65 Temp. L. Rev. 1279, 1282 (1992).

[90] *People* v. *Kevorkian*, 210 Mich. App. 601; 534 N.W.2d 172 (1995) (seeking to enjoin defendant from assisting suicides).

[91] *In re Quinlan*, 355 A. 2d 647 (N.J. 1976), cert. denied, 429 U.S. 922 (1976) (finding a state constitutional right of privacy to terminate artificial life support).

[92] It is a defense to a charge of murder that the defendant's conduct consisted of causing or aiding, without the use of duress or deception, another person to commit suicide. Nothing contained in this section shall constitute a defense to a prosecution for, or preclude a conviction of, manslaughter or any other crime." Or. Rev. Stat. § 163.117 (1995).

[93] See *e.g. The Deceptive Trade Practices Act*, Tex. Bus. & Com. Code Ann. T. 2, Ch. 17 (West 1995); Wash. Rev. Code Ann. § 19.86 (West 1995).

## III. Current Common-law Doctrines Do Not Adequately Protect Individuals' Privacy

The *Restatement (Second) of Torts* describes four distinct actions that constitute an invasion of the right to privacy.[94] The *Restatement* also describes actions for invasions of interest in reputation.[95] Of these five possible deterrent sources, one principle is not applicable to information encoded on identification cards: the appropriation of another's name or likeness as stated in section 652C and it will not be discussed.[96] None of the remaining causes of actions described will provide sufficient remedy to provide a deterrent for the proliferation of information by provided by cards carried by individuals.

*Courts are reluctant to find tortious 'highly offensive' conduct in connection with the use of encoded information.*

Section 652B of the Restatement describes a tort for intrusion upon the seclusion of another,[97] but this tort will not be a viable source of recovery for an individual harmed by a Bellerophontic letter.[98] A prerequisite for recovery would be a "highly

---

[94] 652A. GENERAL PRINCIPLE
(1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.
(2) The right of privacy is invaded by
(a) unreasonable intrusion upon the seclusion of another, as stated in s 652B; or
(b) appropriation of the other's name or likeness, as stated in s 652C; or
(c) unreasonable publicity given to the other's private life, as stated in s 652D; or
(d) publicity that unreasonably places the other in a false light before the public, as stated in s 652E.
*Restatement (Second) of Torts* § 652A (1977).

[95] *Restatement (Second) of Torts* ch 24 (1977) (describing principles of the tort of defamation).

[96] A person obtaining private information from an identification card is not appropriating either the card holder's name or likeness, but merely intercepting information about the cardholder upon presentation of the card by the cardholder.

[97] 652B. INTRUSION UPON SECLUSION
One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. *Restatement (Second) of Torts* § 652B (1977).

[98] Individuals will have difficulty prevailing in an action for intrusion upon seclusion against an entity that collects information from a card offered by the individual. This is true despite the fact that an intrusion "may be by... examination into his private concerns, as by opening his private and personal mail, searching his safe or wallet, examining his private bank account, or compelling him by a forged

offensive" invasion of some intended "solitude or seclusion... or... private affairs or concerns."[99] There is no general authority that a person intends solitude or seclusion of information. Indeed, an individual presenting an identification card is voluntarily offering information and the acceptance of that information can hardly be said to be highly offensive. There is no intrusion where a person locates or supplies information solely for that person's own files.[100] In contrast, an intrusion into a person's physical surroundings is commonly a source of an invasion of privacy. For example, the mere installation of a device capable of overhearing conversations in a bedroom was considered an intrusion, though no actual conversations were heard.[101] In comparison, an invasion of privacy was found in the celebrated case of *Nader* v. *General Motors Corp.*[102] where the defendant was guilty of spying, wire-tapping, eavesdropping, prying into the plaintiff's bank account, and using women to effect an illicit relationship. The difference is the level of activity of the tortfeasor: at one extreme, simply installing the means of intrusion is not enough to effect an invasion, but actual active collection of private information in an unreasonable manner is tortious.

It appears that the use of information encoded on cards will not rise to the level of "highly offensive" action sufficient to represent an intrusion. The court in *Dwyer* v. *American Express Company*[103] found that the activities of the credit card company did not rise to an unacceptable level of behaviour. The defendant credit card company analyzed transactions made by the plaintiff to predict the cardholders' propensity to engage in further purchases, and sold this information to third parties. The activity allowed by the *Dwyer* court can be distinguished from the potential threats to privacy represented by encoded data on an identification card, indicating a need for a deterrent form of action to protect individual's privacy. The transactions

---

court order to permit an inspection of his personal documents." *Restatement (Second) of Torts* § 652B cmt b (1977). In offering the card, the cardholders are offering at least some information about themselves. Ostensibly, this is the reason for offering the card. This was the same reasoning used by the Court in *Dwyer, supra* note 6, holding that the compilation and renting of customer spending patterns voluntarily given to the credit card company was not an unauthorized intrusion.

[99] *Restatement (Second) of Torts* § 652B (1977).

[100] *Tureen* v. *Equifax, Inc.*, 571 F.2d 411 (8th Cir. 1978); *cf. Munley* v. *ISC Financial House, Inc.*, 584 P.2d 1336 (Okla. 1978), asking questions of neighbours is an intrusion.

[101] *Hamberger* v. *Eastman*, 106 N.H.107; 206 A.2d 239 (1964).

[102] *Nader* v. *General Motors Corp.*, 31 A.D.2d 392 (N.Y. App. Div. 1969), aff'd, 255 N.E.2d 765 (N.Y. 1970).

[103] *Supra* note 4.

analyzed by the defendant in *Dwyer* were instances where the credit card holder presented the card for the sole purpose of obtaining credit. The only information the cardholder wished to disclose by presenting the card was the account number. There are no technical reasons that prohibit the design of the credit card or accompanying identification card to convey much more than just the account number. The card itself carries the capability to disclose potential spending patterns by recording a compilation of each item purchased, the location purchased, and the price paid. This information has the potential of putting the card holder at the mercy of the merchant with regard to negotiated prices, since the merchant has the benefit of knowing how much the card holder was willing to pay for a similar item in the past.

It is likely that the court in *Dwyer*[104] would not find an invasion of privacy even where the possessor of the personal information has acted in an even greater level of active information gathering. The *Dwyer* court relied on *Lamont* v. *Commissioner of Motor Vehicles*[105] to hold that "[t]he right to privacy does not extend to the mailbox." Since mailboxes frequently contain various forms of coupons and discounts, it seems unlikely that the court would conclude that the mere securing of a pecuniary advantage by one party to a transaction results in an invasion of privacy to the other party. Theoretically, the individual has the option to not purchase any goods or services using that means of payment. However, with the proliferation of mandatory identification cards, individuals are quickly losing that option. This indicates a need for a means for individuals to protect themselves from an inappropriate acquisition and use of personal information.

*Internal use of encoded information will not be prohibited under section 652D or section 652E, since the information is frequently not given sufficient publicity*

Individuals harmed by Bellerophontic Letters will have difficulty prevailing in an action for publicity given to private life under sections 652D or 652E of the restatement.[106] In order to recover damages under either section, the defendant must

---

[104] *Ibid.*

[105] *Lamont* v. *Commissioner of Motor Vehicles*, 269 F. Supp. 880 (S.D.N.Y. 1969), aff'd, 386 F.2d 449 (2nd Cir. 1967), cert. denied, 391 U.S. 915 (1968).

[106] Section 652D makes an invasion of privacy for publicity given to private life tortious:
652D. PUBLICITY GIVEN TO PRIVATE LIFE
One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that
(a) would be highly offensive to a reasonable person, and
(b) is not of legitimate concern to the public.

give publicity about facts or asserted facts.[107] Generally, a person gathering information from an encoded identification card will not publicize the information: the data will be used only by the person gathering the information for a financial advantage. Arguably, it is the cardholder that is giving the information publicity by circulating the card. It is questionable whether a person who encodes information on the card and hands the card back to the cardholder immediately upon completion of the transaction can be said to have intended a communication to anyone other than the cardholder. Recovery in the actions described by these sections is possible only if the facts gleaned from an identification card are intentionally published to a sufficiently large group.[108] Where the dissemination is to a limited size audience, as is the case if the information is used only by the person collecting the information, the action will fail.[109]

---

652E. PUBLICITY PLACING PERSON IN FALSE LIGHT

One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if

(a) the false light in which the other was placed would be highly offensive to a reasonable person, and

(b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

*Restatement (Second) of Torts* § 652D, 652E (1977).

[107] The comments indicate a difference between the term 'publication' and 'publicity': "'Publication,' in that sense, is a word of art, which includes any communication by the defendant to a third person. 'Publicity,' on the other hand, means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge. The difference is not one of the means of communication, which may be oral, written or by any other means. It is one of a communication that reaches, or is sure to reach, the public. Thus it is not an invasion of the right of privacy, within the rule stated in this Section, to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons. On the other hand, any publication in a newspaper or a magazine, even of small circulation, or in a handbill distributed to a large number of persons, or any broadcast over the radio, or statement made in an address to a large audience, is sufficient to give publicity within the meaning of the term as it is used in this Section. The distinction, in other words, is one between private and public communication." *Restatement (Second) of Torts* § 652D cmt a (1977).

[108] Even when the material is mistakenly given publicity, there is no recovery. For example, in *Wood v. National Computer Systems, Inc.*, 814 F.2d 544, 545 (8th Cir. 1987), test scores of a state mandated test were mistakenly sent to another individual. The court upheld summary judgement for the defendant, reasoning that disclosure to only one other individual did not involve publicity of a highly objectionable nature. Not only is publicity a required element to allow recovery, but the publicity must be intentional.

[109] An insurance company obtained records of a past insurance history from a consumer reporting agency, using them internally to deny coverage. The court held there to be no public disclosure that would give rise to an action for invasion of privacy by public disclosure of private facts. The decision was not unanimous, and the dissent would have held the disclosure "no less 'public' than the posting of a debt in a creditor's shop window." *Tureen* v. *Equifax, Inc.*, 571 F.2d 411 (8th Cir.1978).

*Recovery in an action based on section 652E or on defamation will often be impossible because the information will frequently be true*

The comments indicate quite clearly that recovery under section 652E is predicated on the falsity of the information disclosed.[110] The threat of a defamation action is similarly ineffective to deter dissemination of accurate information.[111] In many circumstances, the information encoded on a card will be accurate. If the information can be shown to be inaccurate, the cardholder may have a successful cause of action. The evidentiary problems presented in pursuing such an action are substantial; not only will the plaintiff be required to show that the information is inaccurate, but that it was the defendant that encoded the false information onto the card. To have damages awarded, the card has to be subsequently presented to others. However, given that the card is returned to the cardholder after transaction is complete, the trier of fact will be challenged with the difficult task of finding the exact source of the inaccurate data. The current state of the common law provides no deterrent to the dissemination of private information through the use of data encoding on identification cards. Without such a deterrent in the form of a common law action, it is more likely that this form of information gathering and dissemination will become increasingly prevalent at the cost of diminished personal privacy. Individuals will be faced with the choice of either foregoing the basic means of interacting in a technological society or accepting frequent disclosures of possibly inaccurate, incomplete, or misleading information about themselves.

## IV. Proposed Safeguards and Final Remarks

Individuals need security in the personal information encoded on identification cards. This security can be conferred by changes to the current statutory or common law. These cards are being used to regulate commerce and social programs. It is unrealistic and fundamentally unfair to require individuals to forgo the benefits of social programs or commercial conveniences to prevent the improper use of personal information. Information encoded on identification cards can be protected with

---

[110] "The form of invasion of privacy covered by the rule stated in [652E] does not depend upon making public any facts concerning the private life of the individual. On the contrary, it is essential to the rule stated in [ 652E] that the matter published concerning the plaintiff *is not true*. The rule stated here is, however, limited to the situation in which the plaintiff is given publicity. On what constitutes publicity and the publicity of application to a simple disclosure, see s 652D, Comment a, which is applicable to the rule stated here." *Restatement (Second) of Torts* § 652E cmt a (1977) [italics added].

[111] "One who publishes a defamatory statement of fact is not subject to liability for defamation if the statement is true." *Restatement (Second) of Torts* § 581A (1977).

either statutory enactments or remedies provided by the common law. Providing a statutory remedy has the advantage of operating proactively. It provides protections in advance of the development of extensive data collection networks that are difficult or expensive to dismantle or change. A statutory enactment protecting all data encoded on cardholders' cards in a manner similar to the protections provided to governmentally held records by the Privacy Act[112] would be effective without interfering with legitimate data encoding purposes. Providing a tort remedy has the effect of deterrence and would have the advantage of adapting quickly to developing technological advancements. A tort remedy has the further advantage of being based on general principles of privacy protection, rather than on possibly imprecise wording of a statute that would quickly become obsolete as technology provides possible loopholes. A safeguard essential to the protection of personal information is one that allows the cardholder to comprehend exactly what information is being released to others.

Data recorded on identification cards must be made available to the cardholder in a comprehensible medium. Any data that is recorded by special machines or devices will remain mysterious to those without access to the needed hardware. Without knowledge about the potential for information to be disclosed, the cardholder does not have the ability to make any meaningful choices about what, if any, personal information is to be disclosed. A cardholder has a legitimate interest in prohibiting the disclosure of information that may be incorrect, incomplete or misleading. These types of disclosure can wreak havoc on the cardholder's life leading possibly to the loss of employment opportunities or the loss of civil or criminal due process.

A partial solution is to allow the release of the information encoded upon the card only to the issuer of the card itself. For a driver's license, this would be only to the appropriate state licensing authority. The system could continue to operate for a legitimate purpose: law enforcement. Once the information is in the hands of the government agency, it would be protected by the Privacy Act. Encoding or reading of the data on the card should be statutorily prohibited with penalties for violations.

A similar solution is possible for information encoded on enhanced Social Security Cards. Cryptographic techniques could be employed to allow data to be encoded onto the card, but with the use of password protection by the issuer of the card in a manner prohibiting reading of the information by unauthorized entities. Where it is necessary to have employers place information on the card, the system

---

[112] 5 U.S.C. § 552a (1995).

should only accept the encoding of such data with the proper password. The cardholder should have the information disclosed upon presentation of the card to the issuing agency and provisions could be made to allow correction or comment by the cardholder on the record in a manner similar to the Privacy Act.[113] Protection of information by allowing access only to the issuing agency would also require a remedy for violation of this requirement. An assessment of civil penalties would be sufficient, although, criminal penalties would be consistent with other forms of electronic interception.[114]

Data encoded on a food stamp debit card is easily protected by statutorily restricting the types of information readable by merchants. There is no conceivable legitimate societal need to allow merchants to gather statistical information from the user of the card. Accordingly, merchants should be prohibited from accessing more than the simple value information needed to complete a sale. The statistical information may have a legitimate use, as for example, in monitoring for potential abuses or fraud. This legitimate purpose can only be affected in the hands of the issuing agency. Once the information is downloaded to their possession, there is no further need for the information to be encoded on the card and it could be erased. Once erased, the data is no longer capable of being circulated by the cardholder. Any system that allows encoding of more than simple value information onto a food stamp debit card should be password protected to prohibit improper disclosure and penalties assessed for improper interception.

The common law should recognize the private nature of information encoded on credit and identification cards as they circulate to effectuate transactions. Obtaining credit is a private matter between the consumer and the issuing company. While it is true that such a relationship is primarily a contractual one, as a practical matter, the consumer has little or no bargaining power to negotiate terms of the agreement. A cardholder may wish to obtain credit, but not wish to be placed at an economic disadvantage unknowingly or erroneously. This should remain the individual's choice as a simple matter of fairness in light of the harm that can come from the disclosure of this information. The common law should reflect the public policy goals evidenced by legislative enactments making certain computer records private. These enactments were in response to the possible harm created by the collection and use of records by the government. New means of collection,

---

[113] *Ibid.*

[114] 18 U.S.C. § 2511(4) (1995) authorizes a sentence of up to 5 years of imprisonment for interception of electronic communications.

compilation, and distribution of those records is possible in a manner that escapes the protections of these statutes. A similar harm can possibly be inflicted by private entities. Without the recognition that certain information about cardholders is private and has the potential to harm people in a direct manner, information will continue to be freely distributed where it generates economic gain for those who control the distribution.

Statutory and common law protections for personal privacy developed over the last century can be circumvented by the use of technological loopholes. The nature of electronically encoded records on identification cards makes them immune and exempt from current protections. In an increasingly mobile and sophisticated society, we leave an increasing number of threads of ourselves in numerous electronic forms. The choice to cut these threads to secure a private life is becoming an increasingly difficult task. It is unrealistic to ask citizens to abandon the benefits of social programs or financial conveniences to secure the right to control over their lives. The consequences of each thread we leave behind cannot be foreseen at the time we create them. The tapestry that may unfold as new means of weaving a picture of the individual is developed may only be decipherable after that picture is revealed and after much irreparable damage has been done.

A driver's license, food stamps or employment opportunities are hardly luxuries. Society cannot fairly deny them to the unlucky few who find that an unfavourable picture of them has been painted without their knowledge, or produced in error, on a data-encoded card. Section 652C of the Restatement (Second) of Torts makes "appropriat[ion]... [of] the name or likeness of another subject to liability... for the invasion of his privacy." Of course, this section speaks of appropriation literally, but the metaphorical is applicable. A person's likeness is protectable because it is unique; it has value when kept unique. The same is true of the history of a person's life: a credit history, a history of trustworthiness in employment, and a law-abiding record. Each has value and, if appropriated, that individual is deprived of basic necessities.

New devices reduce waste, increase efficiency and increase convenience, making them extremely valuable to their owners and developers. When those same devices create more waste, inefficiency and inconvenience, they become destroyers of personal interests. Without knowing exactly what is being lost in eliminating waste, inefficiency or inconvenience, the individual has lost control of determining to what extent private affairs will be disclosed to others. The primary notions of privacy break down in the face of technological advances, thus creating unacceptable results. Personal privacy interests in encoded information must be protected. The alternative is a threat of real harm to real people.

# APPENDIX

(e) Agency requirements -- Each agency that maintains a system of records shall--

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual--

(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include--

(A) the name and location of the system;

(B) the categories of individuals on whom records are maintained in the system;

(C) the categories of records maintained in the system;

(D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;

(E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;

(F) the title and business address of the agency official who is responsible for the system of records;

(G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;

(H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and

(I) the categories of sources of records in the system;

(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;

(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;

(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;

(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;

(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on

whom information is maintained;

(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and

(12) if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

*The Privacy Act of 1974*, 5 U.S.C. § 552a(e) (1995).