

**ARE PERSONAL PRIVACY AND PUBLIC SECURITY ON A COLLISION COURSE?
A CONSTITUTIONAL ANALYSIS OF THE “DRIVER’S LICENSE MODERNIZATION ACT OF 2002”**

Because of public concern over the provisions of H.R. 4633, the “Driver’s License Modernization Act of 2002,” which was sponsored by Representatives James Moran (D-Va.) and Tom Davis (R-Va.) and has been referred to the Committees on Transportation and Infrastructure, Judiciary and Science, The Rutherford Institute is providing an analysis of the legislation.

Located in Charlottesville, Virginia, The Rutherford Institute is an international nonprofit civil liberties and human rights organization dedicated to the defense of constitutional freedoms.

H.R. 4633 seeks to establish standards for State programs for the issuance of drivers’ licenses and identification cards. The Bill targets several serious problems arising out of database abuse and fraud, including identity theft, the market for illicit licenses and identification cards, and underage purchase of alcohol and tobacco products. To combat these and other abuses, the Bill requires each State within five years after the date of enactment to have in effect a driver’s license and identification card program that meets the following requirements:

1. Each license or card shall have an embedded computer chip that i) contains all text data written on the license or card; ii) contains “encoded biometric data matching the holder”; iii) includes encryption and security software and/or hardware that prevents access to stored data without the consent of the holder, “other than access by a Federal, State or local agency (including a law enforcement agency) in carrying out its functions, or by a private agency acting on behalf of a Federal, State or local agency”; iv) accepts data or software from private devices on authorization by the holder; and v) “conform[s] to any other standards issued by [the] Secretary.” § 165(b)(1).
2. States are required to obtain biometric data for the identification of each person to whom a driver’s license or identification card is issued, which shall be “of a type that can be matched to the license or card holder only with the express cooperation of the license or card holder.” § 165(b)(2).
3. States must participate in a federal program linking State motor vehicle databases, in order to provide access by any State to the information contained in the motor vehicle databases of all the States; and each State database shall contain at a minimum i) the data fields

printed on all licenses/cards, “other than the encoded biometric data under section (3)(b)(1)(B)(ii) (“biometric data matching the holder of the license or card”); ii) the biometric data obtained pursuant to section (3)(b)(2)(A); and iii) driver histories, including violations, suspensions and points. § 165(b)(3).

4. States are required to include on licenses and cards “multiple tamper-resistant security features or optical image layers, such as biometric scans, barcodes, 3D, flip, or motion imaging, to assist in visual verification that the license or card is valid.” § 165(b)(4).
5. Finally, each State “shall adopt and implement procedures for accurately documenting the identity and residence of an individual before issuing a driver’s license or identification card.” § 165(b)(5).

The Bill requires the Secretary of Transportation to promulgate guidelines for the States, including standards for the computer chip technology required for compliance with the Bill’s mandates. § 165(c)(1)-(2)(a). The guidelines are to include standards for the ability to network and access information across applications, both public and private, and standards for the encoded biometric data that must be included on each chip. § 165(c)(2)(A)(i)-(ii). In addition, the standards will include “requirements to ensure that such biometric data will be used only for matching the license or card to the presenter and will not be stored in a central database.” § 165(c)(2)(A)(ii). Standards will also be established for the type of information to be contained in the databases, for security features to be placed on licenses/cards, for documentation required of the identity and residence of persons applying for licenses/cards and for a numbering system for State licenses and cards that prevents duplication between States and does not employ Social Security numbers. § 165(c)(2)(C)-(F).

The Bill also provides criminal penalties for any person convicted of making, forging, counterfeiting, mutilating or altering a driver’s license or identification card “with intent that the license or card may be used.” § 4(a), adding Chapter 125 to Title 18, § 2732(1). Penalties are also provided for any person who “tampers with, alters or destroys a computer chip” used in a card or the data contained thereon, *id.*, § 2732(4), or unlawfully “accesses data contained on a computer chip.” *Id.*, § 2732(5). The potential penalties may be severe, ranging from a fine to twenty years’ imprisonment, or both. *Id.*, § 2732.

H.R. 4633 suffers from serious constitutional infirmities and runs directly contrary to established federal public policy in favor of protecting sensitive personal information. This analysis will first address several overarching practical concerns raised by the prospect of electronically monitoring all United States citizens, including potential abuses of such a system, vulnerability to

fraud and theft and the absence of accommodation provided for religious or conscientious objections to imposed participation. The analysis will then address the constitutional issues raised by the Bill, beginning with concerns over the Bill's disregard for the limits of federal authority in matters traditionally within the scope of State authority, then addressing concerns arising from the constitutional right of privacy itself. The analysis will also address apparent conflicts between the provisions of the Bill and federal privacy statutes and the circumvention of the rule-making procedures established by the Administrative Procedures Act.

I. OBJECTIONS TO A NATIONAL ELECTRONIC DATABASE OF CITIZEN INFORMATION

A. Potential Abuse of the Database by Government and Private Individuals and/or Organizations.

Although the Bill ostensibly limits the sharing of information contained in the uniform license or identification card to the purposes intrinsic to those types of cards, experience dictates that use of the card will inevitably expand to include a myriad of governmental and private uses. Already, governmental and private agencies are proposing networking information systems to monitor and screen airline passengers, enable law enforcement authorities to track any citizen and foster a "cashless society." *See, e.g.*, Robert O'Harrow, Jr., *Intricate Screening of Fliers in Works*, *Washington Post*, February 1, 2002, A01; Robert O'Harrow, Jr., *States Devising Plan for High-Tech National Identification Cards*, *Washington Post*, November 3, 2001, A10; Charles J. Murray, *Injectable Chip Opens Door to "Human Bar Code,"* *EETimes*, January 7, 2002, www.eetimes.com/story/OEG20020104S0044; Shelley Emling, *"Smart" Licensing Plan Raises Privacy Concerns*, *Palm Beach Post*, May 6, 2002 (describing use by Boston merchant of driver's license information obtained from bar customers).

B. Vulnerability of the Database.

Perhaps the most critical weakness in the Bill, from the standpoint of improving system security from exploitation and attack, is its lack of definition of the documentary basis that will be required by the Secretary for State issuance of drivers' licenses and identification cards. It has been frequently noted that most or all of the September 11th hijackers entered the country legally and had no criminal record. Further, four of the hijackers easily obtained Virginia drivers' licenses by presenting a notarized declaration of residency, co-signed by a state resident, and a notarized identity form co-signed by a lawyer. O'Harrow, *States Devising Plan, supra*, at A11. Others may have simply obtained Social Security numbers in order to obtain State drivers' licenses. Leigh Strobe, *Policy Changed on Social Security*, *Associated Press*, May 21, 2002 (noting that some September 11th hijackers had falsely obtained Social Security numbers). The only two documents specifically referenced in the

Bill are birth certificates and passports. § 4(a), adding § 2732(3). The former are notoriously easy to falsify, and the latter are held by only a small percentage of the United States population and, thus, are not available for use by most citizens as identification. With the unavailability of Social Security numbers for use as identifiers, *see* § 3(a), adding § 165(c)(2)(F), and the lack of assurances of identity and legitimacy offered by other forms of identification, there is no means of guaranteeing that a person who purports to be a specific individual residing in a specific residence is telling the truth. In fact, the license and identification card system envisioned by H.R. 4633 cannot provide any conceivable safeguards against the kind of fraud perpetrated by the September 11th hijackers or future similar criminal operations.

Nor would the card system provide any real protection against the chief form of financial piracy, which is identity theft. Most identity theft is accomplished by obtaining only two pieces of data, an individual's name and Social Security number. With that information, credit accounts can be established and exploited, then closed; Internet sales transactions can be made in the name of the victim; and confidential financial information of the victim can be accessed. The proposed license and identification card system would not begin to provide safeguards against this growing type of criminal activity.

Further, the proposed identification card system would be vulnerable to computer piracy and "cracking." Because all information would be stored on computer chips installed on cards, the only system that could conceivably ensure complete security of the data housed on the cards would involve data that can be accessed and modified only by governmental agencies, employing proprietary computer-card interface hardware and data reading and encryption software. This kind of secure non-readable system is employed by the United States military and some private employers to assure that access to secure records and offices is authorized. Even this kind of system is not impervious to unauthorized access, however. The very features that would seem to make such a system attractive – universality, reliability and portability – also require that the system be virtually immutable once in place and, therefore, all the more vulnerable to replication of hardware and software systems, reverse engineering and data cracking. *See, e.g.,* John Markoff, *Vulnerability Is Discovered in Security for Smart Cards*, *New York Times*, May 13, 2002, www.nytimes.com/2002/05/13/technology/13SMAR.html (explaining potential means of cracking "smart card" encoded data). The proposed universal identifier system would thus become a Maginot Line of information privacy – a colossal, imposing and expensive system that is powerless to stop data piracy and fraud. In the end, American citizens would be left with an invasive and dangerous government information superstructure – and the enormous tax bill engendered by it – that does not deliver on its promised benefits.

C. Absence of Accommodation for Religious or Conscientious Reasons.

Another serious danger posed by the Bill is the complete lack of accommodation provided for persons who object to using personal identification numbers on religious or philosophical bases. While the number of United States citizens in this category is difficult to ascertain, it could certainly number in the millions, if not the tens of millions. Statutory exemptions from governmental programs requiring the use of identification numbers as a condition to receipt of benefits or privileges are critically important to these individuals, particularly in view of the Supreme Court's reluctance to hold that a constitutional right to accommodation of religious belief on this basis exists. *See, e.g., United States v. Lee*, 455 U.S. 252 (1982) (member of the Old Order Amish failed to withhold Social Security taxes from his farm and carpentry employees as a result of his belief that payment of such taxes and receipt of benefits would violate the Amish faith; no accommodation required); *Bowen v. Roy*, 476 U.S. 693 (1986) (Native American father not entitled to accommodation in federal food stamp program for belief that allowing infant daughter to use a Social Security number would "rob her of her soul"). Congress has traditionally recognized the importance of protecting the religious and spiritual beliefs of all Americans and, thus, has provided statutory exemptions for such persons from various government documentation requirements. *See, e.g.,* IRC § 1402(e)(1) (exemption provided from Social Security taxation for self-employed religious ministers); IRC § 1402(g) (exemption provided from components of self-employment Social Security taxation for members of religious orders traditionally opposed to public relief systems, *e.g.,* Old Order Amish); IRC § 1402(g) (exemption provided where both employer and employee members of religious order traditionally opposed to public relief). A proposal of the magnitude envisioned by H.R. 4633, without accommodation for inevitable dissent and non-participation, has the potential to marginalize, and perhaps criminalize, a substantial portion of the American population or to deprive millions of citizens of governmental services and privileges to which they are entitled.

The Bill also seems misguided in its attempt to criminalize "alteration" or "tampering with" identification cards or the data contained on them without defining those terms. For example, is the addition of private data to a "smart card" for commercial or personal uses, as the system seems to contemplate, potentially unlawful? Would an individual who tapes over the chip or removes it for religious or philosophical reasons be subject to criminal liability? *See United States v. O'Brien*, 391 U.S. 367 (1968) (federal government could constitutionally penalize draft resisters who burned draft cards in protest, provided that action is not targeted at the expressive component of the act); *Wooley v. Maynard*, 430 U.S. 705 (1977) (New Hampshire precluded from enforcing criminal sanctions against persons who covered the motto "Live Free or Die" on State-issued license plates because of their moral and religious beliefs). Criminalization of any individual modification or alteration to the license and identification card system or data without clarifying that such penalties are not

to be applied to expressive conduct in opposition to the system suggests that proponents of the Bill do not believe the federal system created by the Bill can afford to brook dissent.

II. ABSENCE OF CONGRESSIONAL AUTHORITY TO REGULATE STATE DATA COLLECTION PROCEDURES.

In the opinion of The Rutherford Institute, Congress lacks the constitutional authority to pass H.R. 4633. The proposed law commandeers State governments for the purpose of implementing a federal program and thus contravenes the sovereignty of the States. H.R. 4633 is neither a true spending clause provision nor a proper exercise of Congress's power to regulate interstate commerce and, thus, is invalid.

A. Absence of Spending Clause Authority.

While the Bill indicates that it is to be added to Title 23 under the "General Provisions" Subchapter of the "Federal-Aid Highways" Chapter, the wording and operation of the Bill reveal that it is not simply a spending provision. Contrast the language of H.R. 4633 § 165(b), stating that each State *shall* implement the detailed program, with that of, for example, § 165(d)(1), stating that the federal government *may* provide funding for such a program. The wording of the Bill indicates that Congress is issuing a mandate for States to implement the program and merely holding out a possibility that the necessary funds will be provided.

Further, nothing about the language or structure of the Bill suggests that the States must only comply with the Bill's mandates if they wish to obtain the available funding. This fact distinguishes the Bill from others that are clearly appropriate exercises of Congress' spending powers. For instance, consider 23 U.S.C.S. § 153, in which Congress provided an incentive for States to implement laws requiring the use of seat belts and motorcycle helmets. In that statute, Congress simply granted the Secretary the authority to make grants to States that implemented such laws and further provided that States that had not done so by a given date would lose a certain percentage of funds that would otherwise be appropriated to them. The Supreme Court has upheld this use of a "carrot and stick" incentive approach, whereby Congress uses its spending power to further its broad policy objectives. *See South Dakota v. Dole*, 483 U.S. 203 (1987) (indirect imposition of minimum drinking age on States through highway legislation was a valid exercise of Congress's spending power). The Bill in question, however, is not a mere provision of incentives to implement the federal program, but rather a mandate to do so. It is well settled that Congress can neither compel States to enact a federal regulatory program nor command States' officers to administer or enforce such a program. *Printz v. United States*, 521 U.S. 898, 935 (1997).

Further, a key limitation on Congress's use of its spending power is that any conditioning of the provision of federal funds to the States must be unambiguous; States must be able to exercise their choices knowingly. *Id.* at 207; *see also Gebser v. Lago Vista*, 524 U.S. 274 (1998); *Davis v. Monroe County*, 526 U.S. 629 (1999). Far from being "unambiguous," the proposed law is unclear as to what specific actions States must take in order to receive and retain federal funding for the programs and, indeed, is even unclear whether States have any choice to implement the programs. H.R. 4633 appears to be an attempt by Congress to commandeer State governments to enact and enforce a federal regulatory program, which the Constitution does not permit.

In *Reno v. Condon*, 528 U.S. 141 (2000), the Supreme Court drew a distinction between statutes that regulate "State activities," which are constitutionally permissible, and those that seek to control the manner in which States regulate *private citizens*, which are not. *Reno* at 150-51. Undoubtedly, H.R. 4633 seeks to control the manner in which States regulate their citizens by mandating that States must require their citizens to provide certain information as a prerequisite to receiving a State driver's license. The Bill's mandatory language is extremely invasive into the traditional spheres of State authority, purporting to specify by the Secretary's regulations even the particular documentation to be required to establish the identity and residence of applicants. *See Printz v. United States* at 902-903 (striking down Brady Act requirement for national instant background check system to be promulgated by States, including requirements that firearms dealers obtain a "Brady Form" statement with the name, address and date of birth of the proposed transferee and that States verify identity of the transferee); *New York v. United States*, 505 U.S. 144 (1992) (Congress could lawfully provide funding with conditions for State disposal of radioactive waste but could not constitutionally require States to take title to waste). Clearly, H.R. 4633 is not simply a routine exercise of Congress' spending power but is, instead, an apparent undermining of the doctrine of federalism.

B. Absence of Commerce Clause Authority.

The Supreme Court recently addressed the scope of Congress's Commerce Clause power in *Reno v. Condon*, *supra*. The Court's reasoning in *Reno* strongly suggests that the Commerce Clause provides a precarious basis, at best, for H.R. 4633.

Reno upheld the Driver's Privacy Protection Act of 1994 (DPPA), finding it to be a proper exercise of Congress' authority to regulate interstate commerce under the Commerce Clause. *Id.* at 148. Because the DPPA regulated the *sale* of information contained in the records of State Departments of Motor Vehicles (DMVs), it was readily classified by a unanimous Court as a regulation of interstate commerce. Two important distinctions between the DPPA and H.R. 4633 illustrate why the Bill is likely an invalid use of Congress's power

under the Commerce Clause. First, the DPPA's provisions did not apply solely to States but also regulated private persons who obtained the DMV information. *Id.* at 146. H.R. 4633, on the other hand, regulates States alone, rather than market participants in general. Second, the DPPA's regulation of the *sale* of DMV information was clearly a regulation of the information as an item injected into the stream of interstate commerce. *Id.* at 148-149. H.R. 4633 is not a regulation of information as an item in interstate commerce, but rather a mandate requiring States to obtain particular types of information from their citizens as part of their intrastate licensing process. The bill is thus likely to be held invalid as an improper attempt to regulate intrastate, noncommercial activities.

III. THE CONSTITUTIONAL RIGHT OF INFORMATIONAL PRIVACY

By erecting an interstate infrastructure for electronic access to sensitive information currently protected under various provisions of federal law, the intended database contravenes constitutional law and federal policy that protects private information from third party access.

A. History of the Right to Informational Privacy.

The genesis of the right to privacy in American law is generally regarded as an article co-authored by Justice Louis Brandeis and Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). Development of the right continued through various streams of jurisprudence involving the First, Fourth, Ninth and Fourteenth Amendments. The Supreme Court first explicitly recognized a constitutional right to privacy in 1965, in *Griswold v. Connecticut*, 381 U.S. 479, based upon the liberty interest protected by the Due Process Clause of the Fourteenth Amendment. While the Fourteenth Amendment right remained focused on the right of reproductive freedom for some time, *see Eisenstadt v. Baird*, 405 U.S. 438 (1972) ("If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child"); *Roe v. Wade*, 410 U.S. 113 (1973) (stating that right of privacy is "founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action"), the broader implications of the right were also recognized in other contexts, including the receipt and retention of personal information. *See Whalen v. Roe*, 429 U.S. 589 (1977) (recognizing right of privacy as involving avoiding disclosure of personal matters); *Nixon v. Administrator of General Services*, 433 U.S. 425 (1977) (ex-president had a legitimate expectation of privacy in private communications).

The First Amendment has also been held to be a source of the constitutional right to privacy. "If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may

watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds." *Stanley v. Georgia*, 394 U.S. 557, 565 (1969) (Marshall, J.); *Rowan v. United States Post Office*, 397 U.S. 728 (1970) ("right to be let alone" must provide "a sufficient measure of individual autonomy... to permit every householder to exercise control over unwanted mail"). This form of privacy has been interpreted by the federal appellate courts to encompass the right to receive and protect information:

The First Amendment may be implicated where the state compels an individual to speak. If by compelling an individual to reveal information that he would rather keep confidential the state chills the individual's ability to engage in protected speech, the state has infringed the individual's First Amendment right in the protected speech, unless it provides a sufficient justification for the required disclosure.

Denius v. Dunlap, 209 F.3d 944, 954 (7th Cir. 2000). See also cases cited *infra*.

The right to privacy has also been held to emanate from the protections against unreasonable search and seizure of the Fourth Amendment and the right to due process of the Fifth Amendment. Justice Brandeis, in his famous dissent in *Olmstead v. United States*, 277 U.S. 438 (1928), said, "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." *Katz v. United States*, 389 U.S. 347 (1967), overruling *Olmstead* and adopting Brandeis' view, held, "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Further, the level of privacy accorded private information is not affected by recent technological advances that have made it easier to monitor and intercept data. *Kyllo v. United States*, 533 U.S. 27 (2001) (ruling thermal imaging of interior of residence for heat patterns suggestive of marijuana cultivation violated reasonable expectation of privacy).

B. Scope of the Right to Informational Privacy.

The principal federal case involving the constitutional right of informational privacy is *Denius v. Dunlap*, *supra*. In *Denius*, a case handled by The Rutherford Institute, the Seventh Circuit Court of Appeals held that a federal job training program run by the State of Illinois violated the plaintiff employee's right of privacy by requiring him to sign an authorization form permitting access to a broad range of personal records, including medical records, financial records and information related to all civil or criminal legal matters. *Id.* at 949. The Seventh Circuit observed, "[T]he 'concept of ordered liberty' protected by the Fourteenth Amendment's Due Process Clause has been interpreted to include 'the individual interest in avoiding disclosure of personal matters.'" *Id.* at 955, citing *Whalen v. Roe*, 429 U.S. 589,

599-600 (1977); *Nixon v. Administrator of General Servs.*, 433 U.S. at 465 (recognizing “a legitimate expectation of privacy in personal communications”); and *Pesce v. J. Sterling Morton High Sch.*, 830 F.2d 789, 795 (7th Cir. 1987) (“The federal constitution does, of course, protect certain rights of privacy including a right of confidentiality in certain types of information.”). *See also Kallstrom v. City of Columbus*, 136 F.3d 1055 (6th Cir. 1998) (police officers’ privacy interests in address and family member names implicated fundamental liberty interest); *Arakawa v. Sakata*, 133 F.Supp.2d 1223 (D. Haw. 2001) (“the release of a Social Security number potentially rises to the level of a federal constitutional violation, especially when considering the amount of highly personal information that can be recovered as a result of its release”).

The right of informational privacy has been held to extend to medical conditions and treatment. *See Denius v. Dunlap*, *supra*, at 956 (“the right [to privacy] clearly covers medical records and communications”), citing *Anderson v. Romero*, 72 F.3d 518, 522 (7th Cir. 1995) (noting the recognition of this right as early as 1992); *Schail v. Tippecanoe County Sch. Corp.*, 864 F.2d 1309, 1322 n.19 (7th Cir. 1989) (recognizing “a substantial privacy interest in the confidentiality of medical information”); *Doe v. Lockwood*, 1996 U.S. App. LEXIS 19088 (6th Cir. 1996) (public official violated plaintiff’s substantive due process right to privacy concerning husband’s status as HIV-positive individual by disclosing to public); *Mason v. Regional Medical Center of Hopkins Cty.*, 121 F.R.D. 300 (W.Dist. Ky 1988) (status as HIV-positive individual required to be kept confidential in court proceeding). *Cf.* James G. Hodge, Jr., *National Health Information Privacy and New Federalism*, 14 ND J. L. ETHICS & PUB. POL’Y 791 (2000); Eric Wymore, *It’s 1998, Do You Know Where Your Medical Records Are? Medical Record Privacy After the Implementation of the Health Insurance Portability and Accountability Act of 1996*, 19 HAMLINE J. PUB. L. & POL’Y 553 (1998).

The right to informational privacy has also been generally held to extend to financial information. The Seventh Circuit observed in *Denius* that seven of the federal appellate courts had found such a right, while only one had demurred. *Denius*, 209 F.3d at 957. *See Sheets v. Salt Lake County*, 45 F.3d 1383, 1388 (10th Cir. 1995) (finding a constitutionally protected privacy interest in matters concerning “marriage, finances, and business”); *Doe v. City of New York*, 15 F.3d 264, 267 (2d Cir. 1994) (recognizing a constitutionally protected privacy interest in financial information); *Alexander v. Peffer*, 993 F.2d 1348 (8th Cir. 1993) (recognizing a constitutionally protected privacy interest in “highly personal medical or financial information”); *Walls v. City of Petersburg*, 895 F.2d 188, 194 (4th Cir. 1990) (same); *Fraternal Order of Police v. City of Philadelphia*, 812 F.2d 105, 115 (3d Cir. 1987) (same); *Plante v. Gonzalez*, 575 F.2d 1119, 1135 (5th Cir. 1978) (recognizing a “substantial” privacy interest in confidential financial information); *see also James v. City of Douglas*, 941 F.2d 1539, 1543 n.7 (11th Cir. 1991) (recognizing Fifth Circuit precedent in this area finding

a right to privacy in confidential financial information as binding). *But cf. J.P. v. DeSanti*, 653 F.2d 1080, 1090 (6th Cir. 1981) (finding that no right of confidentiality exists under the federal Constitution). The reasons cited for the court's holding that Illinois' stated interests in imposing its employment authorization policy did not override Denius's constitutional right to privacy are cautionary for Congress in light of the lack of statutory safeguards for private information offered in H.R. 4633:

[T]he Authorization provides for the release of a virtually limitless range of confidential financial information. Furthermore, the LCD has provided no basis for requiring this information and no explanation for how it would tailor the gathering of the information to any need it might proffer. Most importantly, the LCD has provided no guarantee that the information obtained pursuant to the Authorization would be kept confidential and only used for a legitimate government purpose. We conclude that this sweeping disclosure requirement, lacking any safeguards against misuse or further disclosure, and supported by no justification, infringes Denius's right of privacy in confidential information.

Id. at 958. The importance of safeguarding the right to privacy of financial information cannot be understated in an increasingly digital economy. As one commentator has noted, “[C]onsumer confidence in electronic money systems will grow as the safety and preservation of important financial privacy rights are guaranteed by regulation.” Bryan S. Schultz, *Electronic Money, Internet Commerce, and the Right to Financial Privacy: A Call for New Federal Guidelines*, 67 U. CIN. L. REV. 779 (Spring 1999).

IV. STATUTORY PROTECTIONS OF THE RIGHT TO INFORMATIONAL PRIVACY

Despite widespread use of the Social Security number as a personal identifier by federal, state and local agencies¹ and historical concerns over identity theft, fraud, illegal immigration and

¹ Numerous federal agencies require the use of the Social Security number besides the Social Security Administration, including the Civil Service Commission, the Internal Revenue Service and the Departments of Defense, Health and Human Services, Justice, Energy, Treasury, State, Interior, Labor and Veterans Affairs. The Tax Reform Act of 1976 gave authority to state or local tax, welfare or general public assistance, and driver's license or motor vehicle registration authorities to use SSNs in order to establish identity. 42 U.S.C. § 405(c)(2)(C)(i) (1976). Not all government agencies, however, are permitted to use an individual's Social Security number or condition benefits on its disclosure. Congress addressed individuals' privacy rights with respect to Social Security numbers in the Privacy Act of 1974, 5 U.S.C. § 552a note; Pub. L. 93-579, § 7, 88 Stat. 1909 (1974). This statute provides that it is “unlawful for any Federal, State, or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to

now terrorism, successive presidential administrations have refused to propose the adoption of a national ID card system. A Social Security Administration task force on the Social Security number rejected extension of the number to the status of an identification card in 1971. Social Security Number Chronology (last updated March 1, 2000) <<http://www.ssa.gov/history/ssn/ssnchron.html>>. A Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems concluded in 1973 that a national identifier was not desirable. *Id.* In 1976, a Federal Advisory Committee on False Identification reached the same conclusion. *Id.* In 1977, the Carter Administration reiterated that the Social Security number was not to become a national identifier, and, in 1981, the Reagan Administration stated that it was explicitly opposed to the creation of an identification card. *Id.* The Clinton Administration also consistently stressed that it was opposed to a national identifier. Electronic Privacy Information Center, National ID Cards (last updated April 17, 2002) <http://www.epic.org/privacy/id_cards/default.html>.

The recognition of a constitutional basis for the right of informational privacy and concerns over the potential abuse of the right engendered by a national identification system have led Congress to codify the right in a number of federal privacy statutes. Various provisions in these statutes prohibit the disclosure of specified private information collected by State or federal agencies, *even to other federal agencies*. Thus, to the extent that H.R. 4633 ostensibly permits the warehousing and sharing of certain personal information collected by States for driver identification purposes, such provisions seemingly violate existing federal law.

The Driver's Privacy Protection Act of 1994. State motor vehicle departments require drivers and automobile owners to provide personal information, which may include a person's name, address, telephone number, vehicle description, medical information, Social Security number and photograph, as a condition of obtaining a driver's license or registering an automobile. *See Reno v. Condon, supra*, 528 U.S. at 143-144. Congress found that many States, in turn, sell this personal information to individuals and businesses for a significant revenue. *Id.* (citing 140 Cong. Rec. 7929 (1994) (remarks of Rep. Goss)). The Driver's Privacy Protection Act of 1994 (DPPA) was enacted in order to establish a regulatory scheme that restricts the States' ability to disclose a driver's personal information without his or her consent. *Id.* at 144. The DPPA regulates the disclosure of personal information contained in the records of State motor vehicle departments (DMVs). *See Reno*, 528 U.S. at 143.

The DPPA generally prohibits any State DMV, or officer, employee, or contractor thereof, from "knowingly disclosing or otherwise making available to any person or entity personal information about any individual obtained by the department in connection with a motor vehicle

disclose his social security account number" *unless* the disclosure is required by federal statute or the agency has required disclosure for identity purposes under a statute or regulation adopted prior to January 1, 1975. *Id.*

record.” 18 U.S.C § 2721(a) (2001). The DPPA defines “personal information” as any 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 not including “information on vehicular accidents, driving violations, and driver’s status.” § 2725(3). A “motor vehicle record” is defined as “any record that pertains to a motor vehicle operator’s permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.” § 2725(1). A 1999 amendment to the Act changed the procedure for consenting to release of information from a mandated “opt-out” system to an “opt-in” system by requiring States to “obtain[] the express consent of the person to whom such personal information pertains.” Act Oct. 9, 1999, subsection (b), in paragraph (11) (effective on 6/1/00). In *Reno*, the Supreme Court upheld the DPPA as consistent with the constitutional principles enunciated in *New York v. United States*, 505 U.S. 144 and *Printz v. United States*, 521 U.S. 898. *Reno*, 528 U.S. at 151.

Right to Financial Privacy Act of 1978. The Right to Financial Privacy Act of 1978 (“RFPA”) was implemented in response to a pattern of government abuse in the area of individual privacy and was intended “to protect the customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity by requiring federal agencies to follow” established procedures when seeking a customer’s financial records. See *Anderson v. La Junta State Bank*, 115 F.3d 756, 758 (10th Cir. 1997); *Clayton Brokerage Co. v. Edward Cement*, 87 F.R.D. 569, 570-71 (Md. 1980). The RFPA was a direct response to the Supreme Court’s unpopular decision in *United States v. Miller*, 425 U.S. 435 (1975), in which the Court declined to extend constitutional privacy protection to financial records maintained by banks, holding that bank customers do not have a reasonable expectation of privacy in their financial records because they voluntarily reveal their financial transactions to banks by availing themselves to banking services. *Id.* at 442-43. The RFPA specifically limited the holding in *Miller* by directly regulating the disclosure of financial records to federal agencies. See Bryan S. Schultz, *Comments: Electronic Money, Internet Commerce, and the Right to Financial Privacy: A Call for New Federal Guidelines*, 67 U. CIN. L. REV. 779, 793-94 (1999).

Under the RFPA, the government may have access to, or obtain copies of, information contained in a customer’s financial records from a financial institution only if the customer authorizes the disclosure, the government obtains an administrative or judicial subpoena or summons or the records are sought pursuant to a search warrant or formal written request. 12 U.S.C. § 3402 (2001); *Anderson*, 115 F.3d at 758. Furthermore, the financial institution may not release the requested financial records until the government “certifies in writing to the financial institution that it has complied with the applicable provisions” of the RFPA, including notice to the customer of the existence of the subpoena, summons, search warrant or request; the nature of the government’s inquiry; and permitting the customer sufficient time to respond to the notice. *Id.*, §§ 3403(b), 3405-08. The Fourth Circuit has held that the Department of the Army violated the plaintiffs’ rights under

the RFPA by examining their American Express card records without their consent. *Duncan v. Belcher*, 813 F.2d 1335 (4th Cir. 1987).

Not only does the RFPA limit the circumstances in which a government may obtain personal financial information, the Act also sets forth strict procedural requirements for the inter-agency exchange of personal financial information already legitimately in the possession of a federal agency. *See Schultz, supra*, at 794. In this way, the RFPA precludes the transfer of financial information between federal agencies unless the government can demonstrate that the receiving agency has a “legitimate law enforcement inquiry” pertaining to the requested records. *See* § 3412(a). The RFPA defines “law enforcement inquiry” as a “lawful investigation or official proceeding inquiring into a violation of, or failure to comply with, any criminal or civil statute or any regulation, rule, or order pursuant thereto.” § 3401(8).

The Social Security Act. The operative privacy provision of the Social Security Act of 1935 is 42 USCS § 1306 (2001). This section prohibits the disclosure of “any return or portion of a return...or of any file, record, report, or other paper, or any information, obtained at any time by the head of the applicable agency (the Social Security Administration or the Department of Health and Human Services) or by any officer or employee... and no disclosure of any such file, record, report, or other paper, or information, obtained at any time by the head of the applicable agency or by any officer or employee of the applicable agency... except as the head of the applicable agency may by regulations prescribe and except as otherwise provided by federal law.” §1306(a). Likewise, the Privacy Act contains protections against required use of the Social Security number to obtain benefits under the Social Security system or as a federal identifier. *See* n. 1, *supra*.

The Electronic Communications Privacy Act. The Electronic Communications Privacy Act (“ECPA”) is part of a detailed legislative scheme enacted as Title III of the Omnibus Crime and Control Act of 1986. *See Adams v. City of Battle Creek*, 250 F.3d 980, 986 (6th Cir. 2001). The legislation seeks to balance privacy rights and law enforcement needs, keeping in mind the protections of the Fourth Amendment against unreasonable search and seizure. *Id.* Congress made the Act the primary vehicle by which to address violations of privacy interests in the communications field. *Id.* In late 1986, Congress expanded the coverage of the anti-wiretapping provisions to provide privacy protection to numerous types of electronic communications and specifically added a definition of “electronic communication” that covered most communications “not carried by sound waves and which cannot fairly be characterized as containing the human voice.” *Id.* Furthermore, Congress amended the “intercept” definition to include the “aural or other acquisition” of “wire, electronic, or oral communication.” *Id.*, 18 U.S.C. § 2510(4). The provisions accordingly reach computer-generated files and communications between computer devices, such as Internet traffic and email.

In addition to expanding the scope of protection granted to electronic communications, the ECPA provides important privacy protection for information stored in electronic databases. *See* 18 U.S.C. § 2510(17). In this way, the Act prohibits most private access to stored electronic communication and often requires the government to obtain a search warrant prior to retrieving stored electronic communications. *Id.* §§ 2701, 2703(a). The protection afforded by the ECPA is largely limited to communications stored for less than 180 days, however, and the government may in fact retrieve information stored for more than 180 days with relative ease. *Id.*

Through statutory provisions such as these, Congress has manifested an intent zealously to protect, and indeed to strengthen, the constitutional right of individuals to be protected against government intrusions on their informational privacy. H.R. 4633 appears to reverse that important policy by mandating that States first acquire specified personal data from their citizens and then make that information available to other various entities. Moreover, any disclosure of medical information (such as driver restrictions and disabilities), financial information or Social Security identification information by the interstate coordination of database information stored pursuant to the proposed Bill would violate numerous federal statutory privacy protections, as discussed above.

V. CIRCUMVENTION OF THE ADMINISTRATIVE PROCEDURES ACT (APA)

Finally, an aspect of H.R. 4633 that is likely to be particularly troubling to citizens who are concerned about government intrusion into their privacy is § 165(c)(4), which removes the rulemaking process triggered by the Bill from the operation of crucial portions of the Administrative Procedures Act. Those sections of the Administrative Procedures Act that the Bill declares inapplicable, 5 U.S.C.S. § 551 et seq., create an operational scheme meant to ensure that agency workings remain both transparent and responsive to the American public.

One such provision is the requirement that agencies publish notice of proposed rulemaking and give the public an opportunity to participate in the process by submitting written comments. 5 U.S.C.S. § 553(b)-(c). The Bill also releases the Secretary's promulgation of guidelines from the otherwise applicable provision that requires most agency meetings to be open to the public. 5 U.S.C.S. § 552b(b). The Bill's removal of the rulemaking process from the specified provisions of the Administrative Procedures Act even releases the agency from the Act's requirement that the agency publish certain information and/or make it available upon request. 5 U.S.C.S. § 552(a).

In considering this aspect of H.R. 4633, it is important to note the important policy objectives achieved by these provisions of the Administrative Procedures Act. "Agency notice must be sufficient to fairly apprise interested parties of the issues involved, so that they may present responsive data or argument relating thereto." Senate Judiciary Committee, *Administrative Procedures Act*, S. REP. NO. 752, 77th Cong., 1st Sess. 14 (1945). This requirement serves both (1) "to reintroduce public participation and fairness to affected parties after governmental authority has

been delegated to unrepresentative agencies;” and (2) to assure that the “agency will have before it the facts and information relevant to a particular administrative problem.” *MCI Telecommunications*, 57 F.3d 1136, 1141 (D.C. Cir. 1995), quoting *National Ass'n of Home Health Agencies v. Schweiker*, 223 U.S. App. D.C. 209, 690 F.2d 932, 949 (D.C. Cir. 1982).

The Bill’s removal of the rulemaking process from the safeguard provided by these portions of the Administrative Procedures Act is likely to heighten public concerns. Citizens may feel that the Bill not only mandates a program that erodes their privacy but also enables a non-elected administrative agency to make determinations behind closed doors about the specific details of the program.