Sarah Zuckerman

Article

PROFITING FROM INFORMATION: FLORIDA'S RIGHT OF PRIVACY AND ITS APPLICATION TO THE SALE AND DISCLOSURE OF PERSONAL INFORMATION

I. Introduction

In 1980 the State of Florida adopted an express constitutional right of privacy,[1] extending to the citizens of the state greater privacy rights than those afforded by the US Constitution. In 1992 Florida adopted the access to public records and meetings proviso, making Florida the only state to have a constitutional provision requiring public access to records.[2] The Florida Statutes also address public policy regarding access to personal information contained in public records.[3] However, despite these explicit provisions, many Floridians have expressed concerns over the control of their personal information, especially the growing collection, sale, and use of sensitive identifiers such as the social security number.

With the growth of the web, abundant personal information including address, telephone number, date of birth, social security number,[4] bankruptcy records, lawsuit records, and property records, is just a few keystrokes away. The internet has become a valuable source of data; some of it useful, some of it intrusive. As the wave of technology washes over our society, local, state, and federal governments have joined in, eager to provide online access to public records. These records make available sensitive personal information collected by government agencies. This availability lends itself to creditors, banks, and

other commercial entities profiting from the sale and exchange of this information.

Many question our constitutional right of privacy and how it applies to protect us from disclosure. What happens when we discover that the state of Florida, which has adopted an express right of privacy, is selling our information as a significant source of revenue for the state? As Justice Overton articulates the dilemma, "How do we protect against abuse or misuse of personal information collected by an entity for one purpose when that entity sells the information to another entity for one or more unrelated purposes without the consent of the individual about whom that information pertains?"[5]

Furthermore, by learning sensitive data about a person, other information is more readily accessible through governmental agencies and private entities, including financial and health information.[6] These disclosures can be used to perpetrate fraud upon a person or otherwise cause great harm to someone and his or her family.[7] Identity theft has become one of the fastest growing crimes in America and Florida ranks among the states with the highest rate of identity theft, led only by New York, California and Texas.[8] Identity theft-related crimes include credit card fraud, banking and retail fraud, and fraudulent loans.[9]

In response to these and other related privacy concerns, the legislature and governor of Florida have commissioned reports on privacy and technology.[10] A main area of focus has been statewide policies relating to the collection, sharing, sale and resale of sensitive personal information held by

government entities.[11] Part II of this note will outline Florida's specific right of privacy and how it applies to the disclosure of personal information. Part III will examine the federal right of privacy and what the federal government is doing to safeguard that right as it affects personal information. Part IV will briefly look at how other states are applying privacy rights to such information. Finally, Part V will propose Florida constitutional and legislative reforms to secure protection from intrusions into private spheres by non-governmental entities.

II. Florida Law

"Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law."[12] Since the voters of Florida adopted an express constitutional privacy provision in 1980, the privacy amendment has been the basis for protecting several types of information and activities from public disclosure.[13] While the first sentence purports to keep government out of our private affairs, the second sentence allows access in by means of public records.

The right to inspect or copy public records (except for exempted records) and an open policy on public meetings is also expressed in the Florida constitution.[14] Furthermore, the Public Records Act[15] operates to make all state, county, and municipal records open for inspection by any person, and includes access by remote electronic means.[16] However, the Act provides

exemptions for certain public records which the legislature has found to be exempt from inspection.[17] Together, these provisions have created a common law right to access and a statutory right to access, both aimed at balancing the two competing interests, opening government to public scrutiny and simultaneously protecting individuals from unwarranted government intrusion.[18]

A. Common Law Right of Public Access

Even before the adoption of article I, section 24, courts were faced with determining whether the Public Records Act exempted only those records provided by statutory law to be confidential, or whether documents confidential or privileged as a result of judicially created privileges of attorney-client and work product were also exempted. This issue was addressed in *B.W. Wait, III v. Florida Power & Light Co.*,[19] where the Supreme Court of Florida held that only public records made confidential by statutory law were exempted.[20] The *Wait* court reasoned that if common law privileges were to be included, the legislature would need to amend the statute, as it was not within the court's power to do so.[21]

In *Forsberg v. Housing Authority of the City of Miami Beach*,[22] constitutional issues were introduced when plaintiffs, tenants in public housing, filed a class action seeking to enjoin the housing authority from allowing public access to information provided by public housing tenants and prospective tenants.[23] Both the circuit court and the Supreme Court of Florida found that the Public Records Act did not violate article I, section 2 of the

Florida constitution nor the first, fourth, fifth, ninth, or fourteenth amendments to the federal constitution.[24] The Court found the housing authority to be an agency whose records are public and no exemption or state constitutional right of privacy operated to shield such records.[25]

In a special concurrence, Justice Overton added that although the records were of a personal and intimate nature, they were not exempted from disclosure by statute, and therefore must be available for public examination to ensure public accountability of the housing authority and its officers.[26] In recognition of Florida's strong commitment to the public's right to know of governmental operations, article I, section 24, makes it clear that courts may not construe the provision in a manner which would impair the public's right of access to public records and meetings.[27] Justice Overton concluded that the public's right to know in these circumstances outweighs any assertion of a state-created privacy right for the public housing tenants.[28]

Four years later, Justice Overton, writing for the majority, articulated these same public access principles as they applied to judicial records.[29] In *Barron v. Florida Freedom Newspapers*, the petitioner, a state senator, filed a motion to seal the court file in a divorce proceeding against his wife.[30] The Supreme Court of Florida held that civil and criminal trials in Florida are public events and adhere to the well established common law right of access to court proceedings and records.[31] Closure of court proceedings or records should only occur when necessary to comply with established public policy set forth in the constitution, statutes, rules, or case law.[32] Although the

constitutional right of privacy established in Florida by the adoption of article I, section 24, could form a constitutional basis for closure in some circumstances,[33] it could not under the facts in the instant case.[34]

The *Barron* standard was utilized subsequently in *Post-Newsweek Stations, Florida Inc. v. Doe*,[35] where the Supreme Court of Florida held that John Does named on the "client list" of an alleged prostitute lacked a privacy interest in their names and addresses and therefore failed to show good cause for prohibiting the public disclosure of such information.[36] The Court stated that once the state gives the information to the defendant, pretrial discovery information attains the status of a public record.[37] However, the public's statutory right of access must be balanced against the Does' constitutional right to privacy.[38] Any right of privacy the Does might have is limited by the circumstances under which they assert that right; "[b]ecause the Does' privacy rights are not implicated when they participate in a crime, we find that closure is not justified under *Barron*."[39]

In a more recent decision, the Supreme Court of Florida determined whether all e-mails transmitted or received by public employees of a government agency are public records pursuant to section 119.011(1) of the Florida Statutes,[40] and article I, section 24(a) of the Florida Constitution,[41] by virtue of their placement on a government-owned computer system.[42] The City of Clearwater maintained a procedure whereby employees reviewed and separated e-mails into two categories, personal and public.[43] A reporter requested access to obtain both personal and public e-mails of two City

employees generated on the City's computers.[44] The Court concluded that personal e-mails fall outside the definition of public records.[45] Mere placement of the e-mails on the City's computer does not make them public records, rather, the e-mails must have been prepared "in connection with official agency business" and be "intended to perpetuate, communicate, or formalize knowledge of some type."[46] The determining factor is the nature of the record, not its physical location."[47]

In interpreting the state constitutional right of privacy as it applies to public access of public records, the courts have served a fundamental role in shaping this area of law. The courts have shown deference to the legislature by finding exemptions for records solely in the statutory law. They have set guidelines for when a person's privacy rights outweigh the public's right to access and the important public policy behind government accountability. Finally, they have demarcated a line between personal and public records within government control. However, given the separation of powers doctrine inherent in our system, we must also analyze how the executive and legislative branches of government have dealt with this doctrine.

B. Statutory Right of Public Access

The general state policy on public records is expressed in chapter 119, Florida's Public Records Act; "all state, county, and municipal records shall be open for personal inspection by any person."[48] The Public Records Act articulates the state's guiding principle on openness and government accountability discussed in the case law. The Act sets out the inspection and

examination of public records,[49] exemptions,[50] a specific social security exemption,[51] remote electronic access to public records,[52] and legislative review of exemptions.[53]

As the case law demonstrated, exemptions to public access of records are created by the legislature and codified in statutory law. The Open Government Sunset Review Act of 1995,[54] details the requirements and process for legislative creation and maintenance of exemptions for public meetings and records.[55] It was through this process that the social security exemption was created.

After a governor commissioned task force on privacy and technology,[56] a House of Representatives Committee Report,[57] and several surveys on the topic were conducted, the Florida Legislature finally recognized the problems in state policies relating to the collection, use, and sale of sensitive personal information. In response, the Social Security Exemption Statute (SSES) was passed. The SSES declares social security numbers (SSNs) held by agencies, employees, or contractors confidential and exempt from section 119.07(1) of the Florida Statutes, and article I, section 24(a) of the state constitution.[58] However, the practical effect of the SSES is very limited.

First, the SSES is undermined by exceptions within the statute. There is an exception to the SSES, stating that SSNs may be disclosed to governmental entities, agents, employees, or contractors if necessary for the entity to perform its duties and responsibilities.[59] Secondly, the SSES states that an agency shall not deny a commercial entity engaged in the performance of a commercial

activity or its agents, employees, or contractors access to SSNs, provided the numbers will only be used in the normal course of business for "legitimate business purposes."[60]

These exceptions to the SSES, especially the latter, open up a huge gap in the wall of defense and effectively limit what little disclosure protection the statute was meant to provide. The "legitimate business purposes" defined in section 3 include a vast list of activities,[61] and represent the private commercial invasions that have become the biggest threat to our privacy today. A feeble attempt to demarcate a limit is made when directly following the list of "legitimate business purposes," the statute says: "A legitimate business purpose does not include the display or bulk sale of social security numbers to the general public or the distribution of such numbers to any customer that is not identifiable by the distributor."[62] However, little to no guidance is given in the SSES to distinguish when something constitutes a "legitimate business purpose" and when it becomes display or bulk sale to the public.

It becomes ambiguous whether the state or its agencies can still display or bulk-sell SSNs to commercial entities who are engaged in a "legitimate business purpose" as defined by the SSES. In addition, because the SSES only regulates disclosure by state agencies, commercial entities that legitimately gain access to SSNs can subsequently resell or disclose this information to whomever they choose, including other commercial entities that do not fall under the "legitimate business purpose" exception of the SSES. These

commercial entities are gaining access to this confidential information and using it for their own purposes, wholly unregulated by the state.

The SSES attempts to address these concerns in section 7 where the Legislature acknowledges that the SSN was never intended for business purposes, can be used as a tool to perpetuate fraud against a person, and to acquire sensitive personal, financial, medical, and familial information, which could cause great financial or personal harm to an individual.[63] The solution to this dilemma: "The Legislature intends to monitor the commercial use of social security numbers held by state agencies in order to maintain a balanced public policy."[64] Section 8 sets out guidelines for agencies; an agency must be authorized by law to collect an individual's SSN and collection must be imperative for the performance of the agency's duties.[65] Finally, rules are given for when the SSN can be displayed on a public record; when a person has the right to request removal of the number from any record; penalties for violation of the statute; and every agency must file a report listing the identity of all commercial entities that requested SSNs during the preceding year and the specific purpose stated by each entity regarding its need for the numbers.[66]

None of these provisions address resale or the subsequent disclosure of information by commercial entities that legitimately gain access; all provisions are directed at state agencies. Furthermore, how feasible is it for the Legislature to monitor every commercial use of the SSN? To illustrate this dilemma, the House Committee on State Administration, in conjunction with the House Committee on Information Technology, conducted a survey

regarding the collection, use, and dissemination of SSNs.[67] All agencies, universities, community colleges, and junior colleges in Florida were surveyed.[68] According to the survey 63% of state agencies and 34% of educational institutions disclose social security numbers when a public records request is made.[69] Fifty nine percent of state agencies and sixty one percent of educational institutions have contracts with non-governmental entities to provide information through which SSNs are disclosed.[70] The state agencies but not the educational institutions receive payment for the disclosure of records containing SSNs; i.e. the Department of Revenue has contracts with private legal service providers, credit reporting agencies, financial institutions, genetic testing companies, BSWA (internet software), and Deloitte and Touche Consulting.[71]

Therefore it seems fool-hardy for the Florida Legislature to presume it can effectively monitor this large range of activity. Nor does it seem the provisions of the SSES effectively restrict the state agencies and educational institutions from their practices and policies. Most likely, stricter provisions than those currently in effect are necessary to restrict state entities and educational institutions from the disclosure and sale of this sensitive personal information.

III. Federal Law

Similar to Florida law, the federal law on disclosure and sale of public records comes from the U.S. Constitution, federal statutes, and case law. Unlike Florida however, the U.S. Constitution does not provide an explicit right

to privacy. The United States Supreme Court has found a limited, implicit right to privacy in our federal constitution.[72] In *Griswold v. Connecticut*, the Supreme Court determined that the Fourteenth Amendment to the Constitution encompasses various "penumbras" or "zones" of privacy rights; under this collection of rights, there dwells a general right of privacy.[73] And yet, the Supreme Court has been careful to make it clear that "the protection of a person's general right to privacy—his right to be let alone by other people—is, like the protection of his property and of his very life, left largely to the law of the individual states."[74] This holding is extremely important because it grants states the primary responsibility of protecting their citizens against private intrusion. Accordingly, most constitutional protections from intrusions in the area of information and privacy will have to come from the states.

Nonetheless, the federal government has not been entirely silent and has continued to develop case law as well as legislation attempting to balance the personal right of privacy against the need for governmental intrusion. As the U.S. Supreme Court case *Whalen v. Roe*[75] demonstrates, federal constitutional issues still arise in the area of privacy. At issue in *Whalen* was whether the state of New York could record in a centralized computer file, names and addresses of persons who had been prescribed certain drugs.[76] Although the district court found that the doctor-patient relationship was one of the zones of privacy accorded constitutional protection,[77] the Supreme Court held that requiring such disclosures to the state having responsibility for the health of the community, does not automatically amount to an impermissible invasion of

privacy.[78] "We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files;" nevertheless, New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy.[79]

The *Whalen* case left much to be desired in the protection of personal privacy and disclosure of sensitive information. In more recent cases, the U.S. Supreme Court has discussed an individual's interest in controlling the dissemination of information in a statutory context, involving the Freedom of Information Act (FOIA). The FOIA was enacted in 1996 to enable an open federal policy on public disclosure, inspection, and examination of public information, including agency rules, opinions, orders, records, and proceedings.[80] The FOIA also provides exemptions, including files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.[81] Just as Florida courts have been asked to interpret the Florida Public Records Act and exercise judicial review of exemptions, the U.S. Supreme Court has had to construe the FOIA and its exemptions.

In *Department of Justice v. Reporters Comm. for Freedom of Press*,[82] the Supreme Court set out several basic principles for interpreting FOIA. First, a court must balance the public interest in disclosure against the interest Congress intended the exemption to protect.[83] Second, the only relevant "public interest in disclosure" to be weighed in this balance is the extent to which disclosure would serve the "core purpose of the FOIA," which is

contributing to public understanding of the operations or activities of the government.[84] Third, whether an invasion of privacy is warranted cannot turn on the purposes for which the request for information is made.[85]

Applying this test to a disclosure request for the names and addresses of union employees, the Supreme Court held that disclosure would constitute a clearly unwarranted invasion of the employees' personal privacy within the meaning of the FOIA.[86] The Court first noted the FOIA reflects "a general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language."[87] The applicable exemption here was exemption 6 which provides that FOIA's disclosure requirements do not apply to "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[88] Under these facts, the Court concluded the relevant public interest supporting disclosure was negligible at best and would reveal little or nothing about the employing agencies or their activities.[89] The FOIA did not require the agencies to divulge union employees' addresses, and the Privacy Act prohibited their release to the unions.[90]

In addition to case law, Congress has created statutory law relating to public information and public records. Following the FOIA, the Privacy Act was enacted in 1974.[91] The Privacy Act applies to the protection of federal government records; forbids the federal government from maintaining secret data banks; and requires the information collected about US citizens to be kept confidential.[92]

An important consumer related statue, the Fair Credit Reporting Act, was passed to ensure accuracy and fairness in credit reporting.[93] Under the Fair Credit Reporting Act, a consumer reporting agency may furnish a consumer report only under the circumstances listed in the Act.[94] These circumstances include employment, licensing, insurance, and to a person with a "legitimate business need."[95] The Fair Credit Reporting Act also allows individual consumers access to their credit report, the opportunity to inspect and correct their credit reports, any information contained within the report, and the sources of that information.[96]

Additionally, Congress has passed the Family Education Rights and Privacy Act to ensure access to education records for students and parents while protecting the privacy of those records.[97] The Right to Financial Privacy Act to prohibit the federal government from examining bank account records without consent or a warrant.[98] The Electronic Communications Privacy Act prohibiting government and law enforcement from monitoring messages sent via public electronic mail.[99] The Video Privacy Protection Act was passed to ban retailers from disclosing the titles of movies rented by customers.[100] Finally, the Children's Online Privacy Protection Act which requires operators of websites directed to children to give notice of information collected and to obtain parental consent for the collection, use, or disclosure of the information.[101]

IV. Laws of Other States

Florida is the only state to have a constitutional provision requiring public access to records.[102] Many states do, however, have statutory provisions governing access to records as well as provisions governing the collection of personal identifying information by agencies.[103] In Maryland, New Hampshire, Nevada, and Pennsylvania, there are no statutory exemptions for SSNs and therefore these states release such numbers to the public.[104] Michigan, Texas, Hawaii, and Ohio all redact SSNs from all public records whether there is a specific public records exemption or not.[105] Other states, including Missouri, Virginia, New York, Oklahoma, and New Jersey have specific statutory exemptions for SSNs contained in records.[106]

For example, New York's Personal Privacy Protection Law addresses the responsibility of state agencies in the collection of personal information.[107] The law requires each agency maintain a system of records which contain only such personal information that is relevant and necessary to accomplish a purpose required by statute or executive order, or to implement a program specifically authorized by law.[108] Oklahoma law provides that no state agency, board, commission, or other unit of state government can request or require that any person reveal his or her SSN in order to obtain services or assistance.[109] Additionally, no Oklahoma state agency, board, commission, or other unit of state government may furnish any information indexed by SSN unless required by law or specifically authorized by the holder of the SSN.[110] New Jersey's Public Records law provides that "a public agency has a responsibility and an obligation to safeguard from public access a citizen's

personal information with which it has been entrusted when disclosure thereof would violate the citizen's reasonable expectation of privacy."[111]

In a novel approach, Wisconsin has created a joint committee on information policy and technology to review information management and technology systems, plans, practices, and policies of state and local governments, their data security and integrity, and their "protection of the personal privacy of individuals who are subjects of databases of state and local governmental agencies and their provision of access to public records."[112] In California, citizens are protected by the Information Practices Act of 1977, which requires each agency to provide on or with any form used to collect personal information from individuals, notice of: the name of the agency requesting the information; the location of the individual's records; the categories of persons who use information in those records; any known or foreseeable disclosures which may be made of the information; and the individual's right of access to records containing personal information which are maintained by the agency.[113]

V. Proposed Solutions

As the U.S. Supreme Court has recognized, an individual's interest in controlling the dissemination of personal information should "not dissolve simply because that information may be available to the public in some form."[114] While both federal and Florida law recognize the growing technological privacy concerns, Florida and its citizens need to take action to

protect those concerns and make sure informational privacy becomes adequately protected.

A. Informing Citizens of their Constitutional and Statutory Rights

One of the principal problems facing the average consumer is lack of awareness of their statutory and constitutional rights. The citizens of Florida need more due process including notice to individuals that commercial entities have such personal information and are utilizing this information freely as a marketable product. Florida citizens should be informed and understand their protections under Florida's privacy amendment and Florida statutes governing disclosure of information. By understanding the legitimate and illegitimate uses for this information, a person can better protect themselves from unwarranted intrusion.

In addition, individuals should know about the Consumer Reporting Act and similar statutes which allow them to access, review and correct such personal information. Awareness includes providing greater access and knowledge of public record correction. The state should also modify credit reporting agency and credit grantors' practices so that the burden of increasing public awareness of the ability to access and correct an individual's credit report, falls on the consumer reporting agencies and not the state.

Finally, Florida citizens should think twice about giving out personal and family information and filling out registration forms without knowing how that information is going to be used. By giving only the minimum required information, inquiring as to how the information will be used, and challenging

the sale, rental, or exchange of personal information to third parties for secondary uses, individuals can take proactive steps to safeguard their privacy.[115]

B. Legislation to Provide Additional Privacy Protections

Although the Florida constitution has an explicit privacy provision, currently, individuals are only protected against government intrusion.[116] Florida could also enact a constitutional amendment which gives its citizens the right to be protected from non-governmental intrusion, i.e. intrusion from private commercial entities and third parties. Then let the legislature create statutory exemptions to the constitutional provision.

C. Focus on Identity Theft

And as an additional safeguard, we need better solutions and more effective ways to address identity theft.[117] Florida and the federal government need to increase the role of law enforcement, provide more prosecution and training of identity theft related crimes, and develop a statewide program for identity theft victims.[118] We also need database protection which would limit access through public records of sensitive personal identifying information, restrict illicit access, and restrict the ability of state entities to provide bulk sale or disclosure of this information.

VI. Conclusion

This note demonstrates there is an additional need for privacy protections under federal and mostly state law. As the information era sweeps technology into every aspect of our lives, our personal information is more and

more suspect to disclosure. An individual's right to protect his or her sensitive personal information becomes more and more difficult and therefore falls onto the state. Especially since the state, has become one of the largest collectors and disseminators of such information. Florida must recognize this special concern and enact constitutional and statutory provisions to reflect this duty.

[1] FL CONST. art. I, § 23.

[2] FL. CONST. art. I, § 24.

[3] FLA. STAT. §§ 119.07(1)(a), 119.15.

[4] Social security numbers were designed originally to help the government keep track of earnings and benefit information and administer Social Security. *See* HOUSE OF REPRESENTATIVES COMM. ON STATE ADMINISTRATION FINAL ANALYSIS (2002). Today, these numbers are used for almost every government transaction and many private transactions, with or without consent. *Id.* Federal and state agencies use the social security number as a person's primary identifier in order to locate records about that person. In addition educational institutions, civil and criminal proceedings, and commercial entities all use the social security number to classify, categorize, and catalog personal information.

[5] Ben F. Overton, Katherine E. Giddings, *The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion*, 25 Fla. St. U. L. Rev. 25, 30 (1997).

[6] HOUSE OF REPRESENTATIVES COMM. ON STATE ADMINISTRATION FINAL ANALYSIS (2002).

[7] *Id.* Laws 2002, c. 2002-256, § 2

[8] Stacey M. McMillian, *Governor Bush Announces Support for Statewide Privacy and Technology Recommendations* (April 3, 2001) *available at* http://www.itflorida.com/press/ 04032001.asp. The city of Miami has the fourth highest number of complaints of cities throughout the US. *Id.*

[9] *Id.* Identity theft is expected to affect more then 750,000 citizens throughout the country with nearly 20 percent of victims reporting theft totaling over $10,000. *Id.* Victims also experience non-monetary harm including a poor credit rating, loan denials and rejection of credit cards. *Id.* Victims of identity theft spend an average of 175 hours attempting to regain their financial health, at a personal cost close to $1,000. *Id.*

[10] HOUSE OF REPRESENTATIVES COMM. ON STATE ADMINISTRATION FINAL ANALYSIS (2002); FLORIDA TASK FORCE ON PRIVACY AND TECHNOLOGY: EXECUTIVE SUMMARY OF POLICY RECOMMENDATIONS (2000).

[11] FLORIDA TASK FORCE ON PRIVACY AND TECHNOLOGY: EXECUTIVE SUMMARY OF POLICY RECOMMENDATIONS (2000).

[12] FLA. CONST. art. I § 23 (1980).

[13] Post-Newsweek Stations, Florida, Inc. v. Doe, 612 So. 2d 549, 552 (Fla. 1992).

[14] FLA. CONST. art. I § 24 (1980). The provision includes records of the legislative, executive, and judicial branches of government, as well as all agencies, departments, and public meetings. §§ 24(a), (b). The only exemptions of records are by law, passed by a two-thirds vote of each house. § 24(c). The law must state the public necessity justifying the exemption and be no broader than necessary. *Id.*

[15] FLA. STAT. § 119.01(1) (1973).

[16] § 119.011(2)

[17] FLA. STAT. § 119.07(3) (1988).

[18] Post-Newsweek Stations, Florida, Inc. v. Doe, 612 So. 2d 549, 552 (Fla. 1992).

[19] 372 So.2d 420 (Fla. 1979).

[20] *Id.* at 424.

[21] *Id. See also* Morgan v. State, 383 So. 2d 744, 746 (Fla. 4th DCA 1980) (only the legislature can create exemptions to the Public Records Act; the courts may not find exceptions by implication); Miami Herald Publishing Co., a division of Knight-Ridder Newspapers v. City of North Miami, 452 So. 2d 572, 573-574 (Fla. 3rd DCA 1984) (the Florida Evidence Code does not exempt from the disclosure requirements of the Public Records Act a lawyer's written communications with his public entity client; if there is to be such an exemption, the legislature is free to enact it); Rose v. D'Alessandro, 380 So. 2d 419, (Fla. 1980) (although there is great concern over keeping state attorney's

investigation confidential, the court followed Wait and reiterated that courts may not pass on the wisdom of legislative determinations).

[22] 455 So. 2d 373 (Fla. 1984).

[23] *Id.*

[24] *Id.*

[25] *Id.* at 374.

[26] *Id.* at 375 (Overton, J., specially concurring). "Florida's constitutional right of privacy does not prohibit the disclosure of tenant files necessary to promote this state's policy of holding governmental agencies, their officials, and their employees publicly accountable." *Id.*

[27] *Forsberg*, 455 So. 2d at 378 (Overton, J., specially concurring).

[28] *Id.* at 379 (Overton, J., specially concurring).

[29] Barron v. Florida Freedom Newspapers, 531 So. 2d 113 (Fla. 1988).

[30] *Id.* at 114.

[31] *Id.* at 116.

[32] *Id.* at 118. The list of circumstances for closure also included: protection of trade secrets; protection of a compelling governmental interest (e.g. national security, confidential informants); to obtain evidence to properly determine legal issues in a case; to avoid substantial injury to innocent third parties; or to avoid substantial injury to a party by disclosure of matters protected by a common law or privacy right not generally inherent in the specific type of civil proceeding sought to be closed. *Id.*

[33] *Forsberg*, 455 So. 2d at 118. The court held that the constitutional right of privacy could form a constitutional basis for closure to avoid substantial injury to innocent third parties (e.g. to protect young witnesses from offensive testimony, or to protect children in a divorce); or to avoid substantial injury to a party by disclosure of matters protected by a common law or privacy right not generally inherent in the specific type of civil proceeding sought to be closed. *Id.*

[34] *Id.*

[35] 612 So. 2d 549 (Fla. 1992).

[36] *Id.* at 550-553.

[37] *Id.* at 551 (quoting Florida Freedom Newspapers, Inc. v. McCrary, 520 So. 2d 32 (Fla. 1988)).

[38] *Id.*

[39] *Id.* at 552-553 (emphasis added).

[40] Chapter 119 defines public records as all documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency. FLA. STAT. § 119.011(1) (1967).

[41] FLA. CONST. art. I, § 24(a). "Every person has the right to inspect or copy any public record made or received in connection with the official business of the state, or persons acting on their behalf, except with respect to records exempted pursuant to this section or specifically made confidential by this Constitution. This section specifically includes the legislative, executive, and judicial branches of government and each agency or department created thereunder; counties, municipalities, districts; and each constitutional officer, board, and commission, or entity created pursuant to law or this constitution."

[42] State v. City of Clearwater, 2003 WL 22097478, *1 (Fla. 2003).

[43] *Id.*

[44] *Id.*

[45] *Id.* at *3.

[46] *Id.* at *4 (quoting Shevin v. Byron, Harless, Schaffer, Reid & Assocs., Inc., 379 So. 2d 633, 640 (Fla. 1980)). "Just as an agency cannot circumvent the Public Records Act by allowing a private entity to maintain physical custody of documents that fall within the definition of 'public records,'[46] private documents cannot be deemed public records solely by virtue of their placement on an agency-owned computer. *Id.*

[47] *Id.* at *5.

[48] FLA. STAT. § 119.01(1) (1995). "The Legislature finds that, given advancements in technology, providing access to public records by remote electronic means is an additional method of access that agencies should strive to provide to the extent feasible." § 119.01(2).

[49] FLA. STAT. § 119.07.

[50] FLA. STAT. §§ 119.07(2), (3); 119.071.

[51] FLA. STAT. § 119.0721.

[52] FLA. STAT. § 119.085.

[53] FLA. STAT. § 119.15.

[54] FLA. STAT. § 119.15(1).

[55] According to the Open Government Sunset Review Act, exemptions are created and maintained for records of a sensitive, personal nature concerning individuals. FLA. STAT. § 119.15(2)(a). Exemptions are also necessary for the effective and efficient administration of a governmental program; or if the exemption affects confidential information concerning an entity. *Id.* Further, the public has a right to access executive branch governmental meetings and records unless the Legislature finds an exemption to be significant enough to override the strong public policy of open government. § 119.15(2). The exemption must serve an identifiable public purpose and may be no broader than is necessary to meet the public purpose it serves. § 119.15(4)(b). An identifiable public purpose is served if the exemption protects information of a sensitive personal nature concerning individuals, the release of such information would be defamatory to such individuals or cause unwarranted damage to the good name or reputation of such individuals or would jeopardize the safety of such individuals; only information that would identify the individuals may be exempted under this section. §§ 119.15(4)(b); (4)(b)(2). Other identifiable public purposes are set forth concerning administration of government; and information of a confidential nature concerning entities. §§ 119.15(4)(b)(1); (4)(b)(3).

[56] FLORIDA TASK FORCE ON PRIVACY AND TECHNOLOGY: EXECUTIVE SUMMARY OF POLICY RECOMMENDATIONS (2000).

[57] HOUSE OF REPRESENTATIVES COMM. ON STATE ADMINISTRATION FINAL ANALYSIS (2002).

[58] FLA. STAT. § 119.0721 (2002).

[59] FLA. STAT. § 119.0721(2). The provision goes on to say that the receiving governmental entity shall maintain the confidential and exempt status of such numbers. *Id.*

[60] FLA. STAT. § 119.0721(3).

[61] *Id.* The list of legitimate business purposes includes verification of accuracy of personal information received by a commercial entity, use in civil or criminal proceedings, use for insurance purposes, use in law enforcement and criminal investigation, use in identifying and preventing fraud, use in matching, verifying or retrieving information, and use in research activities. *Id.*

[62] *Id.*

[63] FLA. STAT. § 119.0721(7) (2002).

[64] *Id.*

[65] FLA. STAT. § 119.0721(8). "Social security numbers collected by an agency must be relevant to the purpose for which collected until and unless the need for social security numbers has been clearly documented." *Id.* The agency should segregate the social security number; upon request, provide a person with a statement of purpose for which the number is being collected and used; the numbers shall not be used by the agency for any purpose other than the purpose stated; if the collection of the social security number is found to be unwarranted, the agency shall immediately discontinue the collection for that purpose. *Id.*

[66] FLA. STAT. §§ 119.0721(5)(a); (5)(b); (4); (6).

[67] COMM. ON STATE ADMINISTRATION AND COMM. ON INFORMATION TECHNOLOGY, DRAFT INTERIM PROJECT REPORT (Nov. 2001).

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] Griswold v. Connecticut, 381 U.S. 479 (1965).

[73] *Id.* at 484-85.

[74] Katz v. United States, 389 U.S. 347, 350-51 (1967).

[75] 429 U.S. 589 (1977).

[76] *Id.* at 591. Specifically, the concern was over drugs having both a lawful an unlawful market, and to prevent the use of stolen or revised prescriptions. *Id.* at 591-92.

[77] *Id.* at 596.

[78] *Id.* at 602.

[79] *Id.* at 605. *But see id.* at 607 (Brennan, J., concurring) "The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology."

[80] 5 U.S.C.A. § 552 (1966).

[81] § 552(b)(6). The Act also provides agency procedures and reporting requirements. *Id.*

[82] 489 U.S. 749 (1989).

[83] *Id.* at 776.

[84] *Id.* at 775. "That purpose, however, is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little of nothing about an agency's own conduct." *Id.* at 773.

[85] *Id.* at 771. Because the privacy interest outweighed the relevant public interest, the Supreme Court held the records at issue were exempted under FOIA's broad disclosure requirements by exemption 7(C). *Id.* at 780.

[86] US Dept. of Defense v. Federal Labor Relations Authority, 510 US 487, 489 (1994).

[87] *Id.* at 494 (quoting Department of Air Force v. Rose, 425 U.S. 352, 360-61 (1976)).

[88] *Id.* at 494-95 (quoting 5 U.S.C.A. § 552(b)(6) (1966)).

[89] *Id.* at 497.

[90] *Id.* at 502.

[91] 5 U.S.C.A. § 552(a).

[92] *Id.*

[93] 15 U.S.C.A. § 1681 (1970). The purpose of the Fair Credit Reporting Act is to "require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy relevancy, and proper utilization of such information…." § 1681(a).

[94] § 1681b(a).

[95] § 1681b(a). A legitimate business need for the information is (i) in connection with a business transaction that is initiated by the consumer; or (ii) to review an account to determine whether the consumer continues to meet the terms of the account. § 1681b(a)(3)(F).

[96] § 1681g. Every consumer reporting agency shall, upon request, clearly and accurately disclose to the consumer:
(1) All information in the consumer's file at the time of the request, except any information concerning credit scores or any other risk scores or predictors relating to the consumer; (2) The sources of the information; (3)(A) Identification of each person that procured a consumer report; (B) An identification of a person under subparagraph (A) shall include-- (i) the name of the person; and (ii) upon request of the consumer, the address and telephone number of the person. § 1681g. The Act also contains an identity theft provision which initiates a fraud alert for any consumer report upon a good

faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft. § 1681c-1.

[97] 20 U.S.C. § 1232g (1994).

[98] 12 U.S.C. § 3401 (1994).

[99] 18 U.S.C. § 2510 (1994). However, this Act contains many exceptions to the general rule forbidding the interception of electronic communication agencies. *Id.*

[100] 18 U.S.C. § 2710 (1992). However, the Act does not prevent the disclosure of the genre of movies the customer rents. *Id.*

[101] 15 USCA § 6502 (1998).

[102] FLA. CONST. art. I, § 24.

[103] HOUSE OF REPRESENTATIVES COMMITTEE ON STATE ADMINISTRATION, FINAL ANALYSIS, at 5 (2002).

[104] *Id.* SSNs are not specifically exempted from public disclosure under Maryland, New Hampshire, Nevada, or Pennsylvania law. *Id.*

[105] *Id.* at 6. Michigan, Texas, and Hawaii all redact SSNs from public records even though there is not a specific exemption under their respective state laws. *Id.* In Ohio there is no statutory exemption for SSNs, but such numbers are still redacted, prior to public disclosure, pursuant to a 1994 Ohio Supreme Court case ruling, State *ex. rel.* Beacon Journal Publishing Company v. City of Akron, 640 N.E. 2d 164 (Ohio, 1994) (holding that employees' SSNs were records for purposes of the Public Records Act, but that disclosure would violate their federal constitutional right to privacy, and harm caused by the invasion of an employee's privacy as a result of the release of that employee's SSN outweighed the public's interest in obtaining such number).

[106] HOUSE OF REPRESENTATIVES COMMITTEE ON STATE ADMINISTRATION, FINAL ANALYSIS, at 6 (2002).

[107] N.Y. PERSONAL PRIVACY PROTECTION LAW, art. 6-A, § 94(a) (1983).

[108] *Id.* In addition, New York law, in regards to the disclosure of personal information, provides that no agency may disclose any records or personal

information unless that disclosure is pursuant to a written request by or the voluntary written consent of the person fo which the records or personal information pertain. N.Y. PERSONAL PRIVACY PROTECTION LAW, art. 6-A, § 96(a) (1983). Finally, personal information is defined in New York's Personal Privacy Protection Act as any information concerning a data subject which, because of name, number, symbol, mark or other identifier, can be used to identify that data subject. N.Y. PERSONAL PRIVACY PROTECTION LAW, art. 6-A, § 92(7) (1983).

[109] OKLA. STAT. § 74-311 (2002).

[110] OKLA. STAT. § 74-3113 (2002).

[111] N.J.S.A § 47-1A-1 (1963).

[112] WIS. STAT. § 13.58 (1997).

[113] CAL. CIV. CODE § 1798.17 (1978).

[114] United States Dep't of Def. v. Federal Lab. Rel. Auth., 510 U.S. 487, 500 (1994).

[115] Other steps individuals can take: ask to be opted-out of direct mailing lists, beware of special offers, pay with cash whenever possible. Ben F. Overton, Katherine E. Giddings, *The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection from Private and Commercial Intrusion*, 25 Fla. St. U. L. Rev. 25, 55 (1997).

[116] FLA. CONST. art. I, § 23.

[117] See Supra notes 6-9 and accompanying text.

[118] One possibility is a statewide clearinghouse for identity theft victims. FLORIDA TASK FORCE ON PRIVACY AND TECHNOLOGY: EXECUTIVE SUMMARY OF POLICY RECOMMENDATIONS (2000). Among many citizens concerns is the inability to find a single contact point to begin the process of reporting incidences of identity theft and starting the identity restoration process. *Id.* The federal government has established a national Identity Theft Hotline and database, and something similar should be started and tailored to the specific concerns of Florida citizens. *Id.* The Task Force recommends legislation to set up: (1) a toll-free hotline for identity theft victims to report incidences and request

assistance; (2) a summary administrative or judicial proceeding through which an individual can legally establish his or her status as an identity theft victim; and (3) the creation of a confidential database of identity theft victims and incidents that can be accessed for law enforcement purposes. *Id.*