April 2005

The Georgia Open Records Law Electronic Signature Exception: The Intersection of Privacy, Technology, and Open Records

Michael L. Van Cise
University of Georgia School of Law

Follow this and additional works at: https://digitalcommons.law.uga.edu/jipl

Part of the Administrative Law Commons, Intellectual Property Law Commons, Internet Law Commons, Law and Society Commons, and the Privacy Law Commons

Recommended Citation
Available at: https://digitalcommons.law.uga.edu/jipl/vol12/iss2/8

This Notes is brought to you for free and open access by Digital Commons @ Georgia Law. It has been accepted for inclusion in Journal of Intellectual Property Law by an authorized editor of Digital Commons @ Georgia Law. Please share how you have benefited from this access. For more information, please contact tstriepe@uga.edu.
THE GEORGIA OPEN RECORDS LAW ELECTRONIC SIGNATURE EXCEPTION: THE INTERSECTION OF PRIVACY, TECHNOLOGY, AND OPEN RECORDS

I. INTRODUCTION

Given modern technology, individuals are legitimately concerned with privacy. Not only does an expansive government bureaucracy collect and store information ranging from financial records to criminal histories, but, in addition, private industry collects volumes of information for marketing and other purposes. Privacy concerns are not new, however. According to Warren and Brandeis, Anglo-American law began recognizing a right of privacy as early as the mid-nineteenth century. In their seminal article, Warren and Brandeis pointed out the need for the formal recognition of a tort remedy for violation of privacy. The Georgia Supreme Court recognized a right of privacy in 1905. If the law was needed to protect against invasions of privacy at the turn of the nineteenth century, protections of privacy are even more critical today when video cameras,

1 Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 213 n.1 (1890) (arguing that the recognition of a right to privacy in tort would not be “judicial legislation” but “merely another application of an existing rule” and citing numerous nineteenth century “privacy” cases based upon property and contract theories); see Michael Hoefges et al., Privacy Rights Versus FOLA Disclosure Policy: The “Uses and Effects” Double Standard in Access to Personally-Identifiable Information in Government Records, 12 WM. & MARY BILL RTS. J. 1, 45-47 (2003) (“The threads of privacy are woven throughout American jurisprudence . . . . Although the Constitution does not provide an explicit right of individual privacy, the Supreme Court has said there is an implied right of privacy grounded primarily in the Bill of Rights, and the Fourteenth Amendment’s ‘concept of personal liberty.’ ”); Jed Rubenfeld, The Right of Privacy, 102 HARV. L. REV. 737, 739 (1989) (arguing that the analysis in privacy cases was focused on the wrong thing in “ask[ing] whether there is a ‘fundamental right’ to perform” the act at issue, and saying that “the fundament of the right to privacy is not to be found in the supposed fundamentality of what the law proscribes [rather] [i]t is to be found in what the law imposes”). Rubenfeld goes on to say, “the right to privacy . . . attaches to the rightholder’s own actions . . . [and] is not informational but substantive, immunizing certain conduct . . . from state proscription or penalty.” Id. at 740.

2 Warren & Brandeis, supra note 1, at 195 (attributing greater invasions into privacy to “[r]ecent inventions and business methods[, . . .] [instantaneous photographs and newspaper enterprise[, . . . and numerous mechanical devices”).

3 See Pavesich v. New England Life Ins. Co., 50 S.E. 68, 71 (Ga. 1905). The court noted that: The right of privacy within certain limits is a right derived from natural law, recognized by the principles of municipal law, and guaranteed to persons in this state both by the Constitutions of the United States and of the state of Georgia, in those provisions which declare that no person shall be deprived of liberty except by due process of law.
camera phones, listening and recording devices, computer databases, the Internet, and changing "business methods" such as increasingly sophisticated data collection practices by marketers make invasions of privacy an almost constant threat.

In addition to awareness of privacy rights, citizens of the United States have long been concerned with transparent government. Political theorists and politicians have long recognized the importance of transparency\(^4\) and believe it critical to the preservation of liberty.\(^5\) As government grew in size, federal and state lawmakers enacted laws to ensure the openness of government and the availability of information to its citizens.\(^6\) Every increase in the size of the government increases the need for access to government information in order to maintain transparency.

These two concerns—privacy and government transparency—are often at odds, but a third concern has added further complexity to this area of the law. This new concern is technology. Lawmakers are concerned with technological advances, such as electronic recordkeeping and electronic commerce (or e-commerce), with good reason. Technology increases efficiency and expands capabilities. Additionally, many expect electronic commerce to become a huge business. According to one estimate, global electronic commerce revenues could reach $6.8 trillion by 2005.\(^7\) This expansion of electronic commerce is the driving force behind electronic signature legislation.

Lawmakers have designed electronic signature laws to foster the continued development and increased use of new technology in the field of electronic contracts and sales. Electronic commerce and advances in technology have come

\(^4\) Letter from James Madison to W.T. Barry (Aug. 4, 1822), reprinted in THE COMPLETE MADISON 337 (Saul K. Padover ed., 1953) ("Knowledge will forever govern ignorance; And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."); see also Hoefges et al., supra note 1, at 9-10 ("Legislators noted that transparent government, subject to public and press scrutiny and evaluation, has a long and historic tradition in the nation.").

\(^5\) John Adams, A Dissertation on the Canon and Feudal Law (1765), quoted in State ex rel. Beacon Journal Publ’g Co. v. City of Akron, 640 N.E.2d 164, 168 (Ohio 1994). President Adams remarked: Liberty cannot be preserved without a general knowledge among the people, who have a right . . . and a desire to know; but besides this, they have a right, an indiscputable, unalienable, indefeasible, divine right to that most dreaded and envied kind of knowledge, I mean of the characters and conduct of their rulers.

\(^6\) See Statement of the President Upon Signing Bill Revising Public Information Provisions of the Administrative Procedure Act, 2 WEEKLY COMP. PRES. DOC. 895 (July 11, 1966) ("[D]emocracy works best when the people have all the information that the security of the Nation permits. No one should be able to pull the curtains of secrecy around decisions which can be revealed without injury to the public interest."). cited in Fred H. Cate et al., The Right to Privacy and the Public’s Right to Know: The “Central Purpose” of the Freedom of Information Act, 46 ADMIN. L. REV. 41, 46 (1994).

\(^7\) Aristotle G. Mirzaian, Electronic Commerce: This is Not Your Father’s Oldsmobile, 26 RUTGERS L. REC. 7 (2002).
so rapidly, however, that the law has been unable to keep pace with such changes.\(^8\) Ironically, problems have arisen from legislators' recognition of the law's inability to keep pace with such rapid changes. The instance at issue in this Note is the negative impact of lawmakers' attempts to pass laws that are technology-neutral on Georgia's open records law. New electronic signature laws, while they may appropriately respond to concerns of rapid changes in technology, have insufficiently dealt with the timeless issues of government transparency and individual privacy.

The term "privacy" has come to embody numerous doctrines in the law. This Note will focus primarily on information privacy, discussing an apparent flaw in the open records law of Georgia. Specifically, the Georgia Legislature recently added a disclosure exception for electronic signatures, an exception which runs counter to the history and purpose of the Georgia open records acts and creates an overly broad exception to the prior law. Georgia has, by implication, created a new privacy exception in its open records law.

II. BACKGROUND

A. ELECTRONIC COMMERCE\(^9\)

The federal government uses the following definition for purposes of government statistics: "E-commerce is any transaction completed over a computer-mediated network that involves the transfer of ownership or rights to use goods or services."\(^10\) Furthermore, the Census Bureau points out that "electronic agreement, not payment, is the key determinant of an e-commerce transaction."\(^11\) The United States Census Bureau estimate of domestic retail electronic commerce sales for just the second quarter of 2004 was $15.7 billion.\(^12\)

Electronic commerce as a percentage of retail sales has increased from 0.7% in

---

\(^{8}\) See, e.g., Sarah E. Roland, The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues?, 35 SUFFOLK U. L. REV. 625, 626 ("The lagging pace of change in the legal system is in stark contrast to the Internet's explosive growth.").


\(^{11}\) Id.

the fourth quarter of 1999 to almost two percent of total retail sales in the first quarter of 2004. While business conducted over a computer does not represent a large portion of the current economy, some expect that it will. Perhaps these expectations are reasonable given the above statistics. In any case, it is with these expectations in mind that legislators have enacted legislation to further the growth of electronic commerce both domestically and globally.

B. ELECTRONIC AND DIGITAL SIGNATURES

1. Definition of Terms. A signature is “[a]ny name, mark, or writing used with the intention of authenticating a document.” An electronic signature is defined by the Uniform Electronic Transactions Act (UETA) as “the execution of a sound, symbol or process with the intent to sign.” In contrast to a traditional

13 Id.
14 See Mirzaian, supra note 7 (“[W]orldwide e-commerce revenues are expected to reach $6.8 trillion by 2005.”).
15 See, e.g., Julian Epstein, Cleaning up a Mess on the Web: A Comparison of Federal and State Digital Signature Laws, 5 N.Y.U. J. LEGIS. & PUB. POL’Y 491. President Clinton stated: The [E-Sign] Act will open up new frontiers of economic opportunity . . . . The new law will give fresh momentum to what is already the longest economic expansion in our history, an expansion driven largely by the phenomenal growth in information technologies, particularly the Internet . . . . [P]roductivity gains are rippling throughout our economy . . . . Perhaps no invention since the railroad has had such potential to expand our opportunities and broaden our horizons—I would argue, more profound potential.

Gregory Todd Jones, Electronic Signatures and Records: Permit the Use of Electronic Signatures and Records Even When a Statute, Regulation, or Other Rule of Law Specifies a Non-Electronic Type of Signature or Record 18 GA. ST. U. L. REV. 6, 7 (2001) (“[A] troubling question remained for states across the nation which were grappling with the issue of evolving electronic transactions. With the speed of technological innovation, how would one define an electronic signature in such a way as to promote innovation.”).

While the terminology can be confusing, it is critical to an understanding of the law and the topics discussed in this Note. See Mirzaian, supra note 7, at Section (II)(A)(4)(a) (“The terms ‘digital signature’ and ‘electronic signature’ are often confused because of the common misconception that they are synonymous.”).

17 UNIF. ELEC. TRANSACTIONS ACT § 2(8) (1999), available at http://www.law.penn.edu/bll/ulc/fnact99/1990s/ueta99.htm. Comment 7 to the UETA definition of the term “electronic signature” is helpful. It states, “No specific technology need be used in order to create a valid signature.” Id. Furthermore, Comment 7 explains that a voice on an answering machine, a name as part of an electronic mail communication, or even the firm name on a facsimile, could each be an electronic signature when paired with the requisite intention. Id.; see also O.C.G.A. § 10-12-3 (2000) (“‘Electronic signature’ means a signature created, transmitted, received, or stored by electronic means” and “‘Electronic’ means, without limitation, analog, digital, electronic, magnetic, mechanical, optical, chemical, electromagnetic, electromechanical, electrochemical, or other similar means.”).
signature and an electronic signature, a digital signature is not really a signature at all because it does not require intent. Rather, a digital signature is a specific technology used to provide assurance that the message sent is not intercepted or compromised en route to the intended recipient and that identifies and authenticates the sender. 19 It is important to recognize that a digital signature can be an electronic signature when that digital signature is used with the intent to sign.

2. Electronic and Digital Signature Legislation. The Utah Digital Signatures Act, adopted in 1995, was the first piece of legislation designed to create a standard for electronic signatures. 20 The Utah legislature chose to enact laws giving validity only to cryptography-based digital signatures 21 as opposed to other state legislatures that created broad, technology-neutral electronic signature laws. 22 Soon after the passage of the Utah act, New York adopted a similar standard in its Electronic Signatures and Records Act. 23 The American Bar Association’s Digital Signature Guidelines, 24 while not intended to serve as a model for a digital signature statute, had an impact on legislatures passing electronic signature laws. 25

19 See American Bar Association, Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, available at http://www.abanet.org/scitech/ec/isc/dsg-toc.html. The term “Digital Signature” has been defined as “[a] secure digital code attached to an electronically transmitted message that uniquely identifies and authenticates the sender.” Black’s Law Dictionary, supra note 17, at 1415; see also Thomas J. Smedinghoff & Ruth Hill Bro, Moving With Change: Electronic Signature Legislation as a Vehicle Advancing E-Commerce, 17 J. Marshall J. Computer & Info. L. 723, 730-31 (1999) (“ ‘Digital signature’ is simply a term for one technology-specific type of electronic signature. It involves the use of public key cryptography to ‘sign’ a message, and is perhaps the one type of electronic signature that has generated the most business and technical efforts, as well as legislative responses.”); Unif. Elec. Transactions Act, supra note 18, cmt. 7 (revealing that the primary distinction between an electronic and digital signature is that “[o]ne may use a digital signature with the requisite intention, or one may use the private key solely as an access device with no intention to sign, or otherwise accomplish a legally binding act”). Put simply, a digital signature involves the use of specific technology to verify and decrypt a record, whereas an electronic signature involves some electronic symbol, which might be a digital signature, and intent.

20 Utah Code Ann. §§ 46-3-101 to 46-3-504 (1999); Roland, supra note 8; Smedinghoff & Bro, supra note 19, at 726.

21 Utah Code Ann. §§ 46-3-101 to -504; Smedinghoff & Bro, supra note 19, at 725.

22 See supra note 18 and accompanying text and infra notes 26, 28, 31 and accompanying text (discussing E-Sign, UETA, the Florida Electronic Signatures Act, and the Georgia Electronic Records and Signatures Act).


24 American Bar Association, supra note 19.

25 Id. at 20; Edward D. Kania, The ABA’s Digital Signature Guidelines: An Imperfect Solution to Digital Signatures on the Internet, 7 Common L. Conspectus 297, 301, 304 (1999); Smedinghoff & Bro, supra note 19, at 726.
and may have contributed to the adoption of digital signatures as the only accepted means of validating a contract by electronic signature.

In contrast to Utah, Florida and Georgia passed less restrictive legislation. The Florida legislature recognized both digital signatures and electronic signatures in their broader sense in its Electronic Signature Act of 1996 and has since adopted the similarly broad UETA. Georgia also enacted general electronic signature legislation not restricted solely to electronic signatures adopted using digital signature protocol. After the aforementioned state laws, the National Conference of Commissioners of Uniform State Laws created the UETA, employing a general, technology-neutral standard similar to the standard applied by the Georgia and Florida legislatures.

In 1999, the federal government considered legislation similar to that of Utah and New York but never passed the bill. In 2000, the federal government took action by passing the Electronic Signatures in Global and National Commerce Act (E-Sign Act). To some extent, this federal legislation creates a national standard for electronic signature legislation. The E-Sign Act contains a limited, express preemption of state law. States may avoid preemption by adopting the UETA. States may have unique legislation only to the extent that the state law is

---

29 UNIF. ELEC. TRANSACTIONS ACT, supra note 18.
30 Roland, supra note 8, at 630; see Digital Signature Act of 1999, H.R. 1572, 106th Cong. (1st Sess. 1999).
E-Sign contains an unusual form of a limited, express preemption of state law. Rather than providing that the federal law preempts all inconsistent state laws, E-Sign sets forth the limited circumstances in which state laws will not be preempted. E-Sign explicitly does not preempt a state enactment ... that adopts the official version of the Uniform Act. A departure from the official version may avoid preemption if it is consistent with the substantive provisions of E-Sign and is technology neutral.
33 Id.; see also 15 U.S.C. § 7002(a)(1) (preceding the requirements with, “A State ... may modify, limit, or supersede the provisions of section 7001 of this title with respect to State law only if such statute, regulation, or rule of law”) (emphasis added).
technology-neutral and does not conflict with the E-Sign Act. The important portion of the E-Sign Act in relation to state electronic transaction law is as follows:

[W]ith respect to any transaction in or affecting interstate or foreign commerce—(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

After the mandate of the E-Sign Act, legislation must be technology-neutral with respect to electronic signature legislation. The rationale behind the requirement of technology-neutral legislation is that, in order for private industry to invest in the development of better technology, it is critical that the law not favor one specific technology such as digital signature technology.

C. OPEN RECORDS LAWS: HISTORY AND POLICY

Assistant Attorney Generals Cohen and Manis announced that “[g]ood government has become increasingly synonymous with open government . . .” Open records laws make government documents and information available to the

35 Id. § 7002(a) (defining the technology neutral requirement in § 7002(a)(2)(A)(ii)); see, e.g., O.C.G.A. § 10-12-2(b) (Supp. 2004) (“The General Assembly finds that this chapter is consistent with [E-Sign] . . . and therefore continues to have the full force of law. The General Assembly further reaffirms its intent that this chapter continue to have the full force of law.”).


37 15 U.S.C. § 7002(a). The statute states that:

[A] State statute, regulation or other rule of law may modify, limit, or supersede the provisions of section 7001 of this title with respect to State law only if such statute, regulation, or rule of law [enacts the UETA or] specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, if . . . such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures.

38 Smedinghoff & Bro, supra note 19, at 761.

public and attempt to encourage public access to government information to increase "public awareness about the decision making process." At the same time, these laws recognize that some limits are necessary to prevent disclosures that might threaten the decisionmaking process itself.

Professor Daniel Solove describes four general functions of government transparency as provided through open records law. First, transparency facilitates public knowledge and understanding of the government and its functions. Second, transparency makes information about government officials available that, in turn, allows the public to examine and evaluate government activity. Third, transparency facilitates social transactions. For example, public records are needed to enable transfer of real property because transparency allows people to trace ownership and title in land. Fourth, transparency makes gathering personal information possible for other purposes. For example, law enforcement officials use public records to locate criminals and "deadbeat parents" and to investigate crimes, parents use public records to investigate babysitters or child care professionals, and employers use public records to screen potential employees.

Exceptions to disclosure exist not only to protect the functions of government but also to protect privacy. Many open government statutes are modified on a

---

41 Cohen & Manis, supra note 39, at 2; see, e.g., Cate et al., supra note 6, at 65 ("The FOIA was designed to protect and advance three goals: first and most important, ensure public access to the information necessary to evaluate the conduct of government officials; second, ensure public access to information concerning public policy; and third, protect against secret laws, rules and decisionmaking.").
42 Cohen & Manis, supra note 39, at 2.
44 Id. at 1173-75. Professor Solove writes:
By promoting awareness of the workings of government, transparency serves a "watchdog" function . . . Courts and commentators have pointed out that the Watergate Scandal might never have been uncovered if the original bail hearing had been closed to the press because reporters . . . would not have been suspicious that expensive attorneys were representing the burglars.
45 Id. at 1175.
46 Id. (giving other examples and specifically noting that "[p]ublic record information is useful in locating witnesses for judicial proceedings as well as locating heirs to estates"). Solove goes on to state that "[A]ccess to public records can allow individuals and entities to track down individuals they want to sue and to obtain the necessary information to serve them with process." Id.
47 Id.
48 Id. at 1175-76.
regular basis,\textsuperscript{50} which indicates that privacy may be the motivating factor more often than concerns about protecting the functions of government.

1. \textit{Federal Law}. The Administrative Procedure Act\textsuperscript{51} governed requests for federal records until the passage of the Freedom of Information Act (FOIA) in 1966.\textsuperscript{52} In the year following its passage, the original FOIA was amended to include nine categories of exemption.\textsuperscript{53} Federal courts initially allowed federal agencies to apply the exceptions broadly,\textsuperscript{54} but following the Watergate scandal, Congress expressed its discontent over such broad application by amending the FOIA in 1974.\textsuperscript{55} Congress further amended the FOIA in 1976, 1981, and 1986.\textsuperscript{56} In 1996, Congress passed the Electronic Freedom of Information Act that mandated access to agency records contained in databases.\textsuperscript{57}

Congress expressed the purpose of the FOIA as follows:

\begin{quote}
[T]he purpose . . . is to require agencies of the Federal Government to make certain agency information available for public inspection and copying and to establish and enable enforcement of the right of any person to obtain access to the records of such agencies, subject to statutory exemptions, for any public or private purpose.\textsuperscript{58}
\end{quote}
2. Florida Open Records Law. Even though Florida codified its public records law after the passage of the FOIA, "a legislative policy on public records can be traced back... to at least 1909." In 1985, the attorney general of Florida wrote, "The government of Florida has been one of the most open anywhere in the world since the enactment of a more comprehensive open meetings law and public records law in 1967." This seems to remain true today, as Florida has expressly supported the move to electronic record keeping and stated its intent not to limit public access. In 2004, Florida updated its statement on electronic record keeping. To further the state policy "that all state, county, and municipal records [shall be] open for personal inspection by any person," Florida provides for immediate hearing of actions filed, requires agencies to comply with court orders within forty-eight hours, and only allows for stay orders when making records public "will result in significant damage." Even when an exemption applies, government agencies must produce the record, redacting only the portions of the record to which an exemption applies. When not producing the complete record, the agency representative must "state the basis of the exemption... including the statutory citation... and, if requested by the person seeking the right under this subsection to inspect, examine, or copy the record, etc.

60 Jim Smith, The Public Records Law and the Sunshine Law: No Attorney-Client Privilege Per Se, and Limited Attorney Work Product Exemption, 14 STETSON L. REV. 493, 494 n.3 (1985) (stating that "1909 Fla. Laws 5942 provided in pertinent part that all state, county and municipal records shall at all times be open for a personal inspection, and that the penalty for violation of the act was removal or impeachment").
61 Id. at 493; see also Paul M. Schwartz, Privacy and Participation: Personal Information and Public Sector Regulation in the United States, 80 IOWA L. REV. 553, 607 (1995) (pointing out that the Florida constitution explicitly makes open government statutes superior to its state constitutional right of privacy).
62 See FLA. STAT. ANN. § 119.01, superseded by FLA. STAT. ANN. § 119.01 (Supp. 2005) (effective Oct. 1, 2004). The statute states:
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 [and]... that automation of public records must not erode the right of access to those records. As each agency increases its use of and dependence on electronic recordkeeping, each agency must ensure reasonable access to records electronically maintained. See also Martin E. Halstuk, Shielding Private Lives from Prying Eyes: The Escalating Conflict Between Constitutional Privacy and the Accountability Principle of Democracy, 11 COMMON L. CONSPECTUS 71, 94 (2003) (stating that Florida open records laws have been regarded as a model for other states).
63 FLA. STAT. ANN. § 119.01 (giving guidance on issues not addressed in the prior law such as providing data in a common format).
64 Id. § 119.01(1).
65 Id. § 119.11.
66 Id. § 119.07(1)(b).
ELECTRONIC SIGNATURE EXCEPTION

[the agency representative] shall state in writing and with particularity the reasons for the conclusion that the record is exempt."\(^{67}\)

Despite its policies favorable to government transparency, Florida does have restrictions on access to public records.\(^ {68}\) These exemptions include "[t]he home addresses, telephone numbers, social security numbers, and photographs of active or former law enforcement personnel"\(^ {69}\) as well as phone company records that include personal information.\(^ {70}\) Indicative of the change inherent in this field of law is the fact that Florida has amended the portion of its open record law that provides for exceptions every year from 1977 to 2004.\(^ {71}\)

3. Ohio Open Records Law. In 1963, the Ohio open records statute codified "an emerging common law rule" that granted access to public records.\(^ {72}\) Ohio's Public Records Act, like Florida's, provides rules to ensure access to public records.\(^ {73}\) Ohio law defines public records broadly and has only a few disclosure limitations, which Ohio courts interpret strictly.\(^ {74}\) Despite Ohio's tendency to liberally disclose records, the state supreme court in *Beacon Journal Publishing Co. v. City of Akron* held that although Ohio had no social security number exception, the U.S. Constitution mandated such an exception to the Public Records Law.\(^ {75}\)

\(^{67}\) Id.

\(^{68}\) See id. § 119.07(6)(a)–(6)(jj) (defining the records and information exempt from disclosure under the law); Mary K. Kraemer, *Exceptions to the Sunshine Law and the Public Records Law: Have They Impaired Open Government in Florida?*, 8 FLA. ST. U. L. REV. 265, 280-94 (1980).

\(^{69}\) FLA. STAT. ANN. § 119.07(6)(i)(1).

\(^{70}\) Id. § 119.07(6)(e).

\(^{71}\) Id. § 119.07.


\(^{73}\) Id. at 116 (stating that Ohio's Public Records Act is "within the most liberal class of public records acts").

\(^{74}\) Id.; *State ex rel. Lindsay v. Dwyer*, 670 N.E.2d 1375 (Ohio Ct. App. 1996) ("[P]ublic policy . . . requires a liberal construction of provisions defining public records and a strict construction of the exceptions.").

\(^{75}\) 640 N.E.2d 164 (Ohio 1994). The court stated:

\begin{quote}
We find today that the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs. Our holding . . . is intended to preserve one of the fundamental principles of American constitutional law—ours is a government of limited power. We conclude that the United States Constitution forbids disclosure under the circumstances of this case.
\end{quote}

*But see State ex rel. Beacon Journal Publ'g Co. v. City of Akron*, 640 N.E.2d 164, 170, 172 (Ohio 1994) (Douglas, J., dissenting) (arguing that the majority had no legal authority for its decision and was engaging in judicial activism). In his dissent, Justice Douglas pointed out that the majority cited neither Ohio law nor any federal statute or provision of the U.S. Constitution. *Id.* He further argued that the majority's balancing of interests was contrary to Ohio law because it is the legislature's role to "balance the competing concerns of the public's right to know and individual citizens' right to
4. **Georgia Open Records Law.** Although Georgia has had an open records act since 1959,76 the Georgia Legislature did not define the term “public records” until 1988,77 indicating that Georgia was not necessarily the leader in the development of open records law.

The stated purpose of the Georgia Open Records Act is “to encourage public access to government information and to foster confidence in government through openness to the public.”78 Even in the wake of the Supreme Court’s holding that the FOIA does not require disclosure of criminal information “rap sheets,” Georgia amended its law to provide for the disclosure of that information.79 Unlike the FOIA, however, the Georgia Open Records Act “mandates the nondisclosure” of information excepted by the Act.80 This reveals that Georgia has stronger privacy protection than the federal government,81 at least as far as government agencies releasing information to requesters of open records is concerned.

D. GOVERNMENT INFORMATION COLLECTION AND PUBLIC RECORDS: INCREASE IN GOVERNMENT SIZE AND ADVANCE IN TECHNOLOGY

The federal government collects revenue, funds social welfare programs, and regulates many aspects of the lives of its citizens.82 In order to effectively complete these tasks, the government must collect volumes of personal information.83 State governments perform similar tasks, which also require the keep private certain information that becomes part of the records of public offices” and chose not to provide a social security number exception to the Public Records Law even though it had addressed social security numbers in other portions of the code.  

76 Cohen & Manis, supra note 39, at 3.

77 Id.


79 Beall, supra note 6, at 1293-94 (“Under the 1995 Amendments, the Georgia legislature has made a policy choice to favor disclosure—albeit limited disclosure—over privacy.”); see also 1995 Ga. Laws 633 (act to amend the law relating to the Georgia Crime Information Center).

80 Bowers v. Shelton, 453 S.E.2d 741, 743 (Ga. 1995) (emphasis removed) (citing Harris v. Cox Enters., Inc., 348 S.E.2d 448 (1986)); see also Schwartz, supra note 61, at 593 (“An essential concept regarding the FOIA is that it sometimes requires the government to disclose information, but never requires nondisclosure.”); Solove, supra note 43, at 1162 (“FOIA does not require that the government withhold information.”).

81 But see Schwartz, supra note 61, at 593-94 (indicating that the Privacy Act can block disclosure to a third party even though the FOIA does not require disclosure).


83 Whalen v. Roe, 429 U.S. 589, 605 (1989) (“The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and
collection of personal information. Open records laws make much of this information public.

Prior to advances in technology such as databases and the Internet, requesters of government documents had to visit the governmental department that held the record sought, identify the record or information requested, and then hope that the record or information could be located. Assuming the agency could fulfill the request, the requester would then examine the record, perhaps make a copy, and return the record. Today, information is much more available, both in the form of electronic databases at governmental agencies and on the Internet.

the enforcement of the criminal laws all require the orderly preservation of great quantities of information.

See Solove, supra note 43, at 1143-44; Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 STAN. L. REV. 1393, 1403 (2001) ("States maintain public records of arrests, births, criminal proceedings, marriages, divorces, property ownership, voter registration, workers compensation, and scores of other types of records. State licensing regimes mandate that records be kept on numerous professionals such as doctors, lawyers, engineers, insurance agents, nurses, police, accountants, and teachers."). For example, State Motor Vehicle Departments collect personal information that, prior to the passage of the Driver's Privacy Protection Act (DPPA), many states sold to private entities. See infra note 107.

See supra text accompanying notes 40-41, 43.

Rosemary Barnes, Technology; Snooping Online is Big Business; Increased Access to Online Information Has Given Birth to Firms Specializing in Cataloging and Selling Public Information, SAN ANTONIO EXPRESS NEWS, Aug. 28, 2004, at 7H; Jackson, supra note 72, at 110; Solove, supra note 43, at 1139.

Hoefges et al., supra note 1, at 5 ("While technology can make access to electronically-stored information faster and cheaper, it can also make invasions of personal privacy far easier.").

At least one state legislature has mandated the placement of public records on the Internet. See ARIZ. REV. STAT. ANN. § 10-122 (2005), which states:

The commission shall administer the [public access] fund and spend monies in the fund to purchase, install and maintain an improved data processing system .... The data processing system shall be designed to allow direct, on-line access by any person at a remote location to all public records that are filed with the commission pursuant to this title and title 29, chapter 4.

Numerous states permit records to be made available by remote access. See, e.g., FLA. STAT. ANN. § 119.01(e); KY. REV. STAT. ANN. § 61.874(6) (2001); MD. CODE ANN., Maryland Rules, § 16-1008(a)(2)(D) (2005); 65 PA. CONS. STAT. ANN. § 66.2(d) (2005) ("[A]n agency may make its public records available through any publicly accessible electronic means."); S.D. CODIFIED LAWS § 15-15A-11(1) (2004) (court records); VA. CODE ANN. § 58.1-3122.2 (2004) ("The commissioner of the revenue may provide remote access, including access through the global information system known as the Internet, to all nonconfidential public records maintained by his office."). Georgia does not require public records to be on the Internet, but personally identifiable information is easily accessible. See, e.g., Letter from Russell W. Hinton, State Auditor, Department of Audits and Accounts to the General Assembly, available at http://www.audits.state.ga.us/esa/index.html (allowing access to salary and travel reimbursement information for state employees simply by clicking "I understand: Proceed to the Salary and Travel Supplement" link at the bottom of the page); see also GUIDESTAR: THE NATIONAL DATABASE OF NONPROFIT CORPORATIONS, at http://
The requester can now acquire the same information at a lower cost and in far less time.\textsuperscript{90} Requesters can collect and sort large volumes of information in a fashion that would not have been possible if requesters were required to look through paper files.\textsuperscript{91} Since the advent of the Internet, a person can search online databases of public information that were previously legally available in paper form but were, for all practical purposes, unavailable to all but the most diligent. The fact that information is stored electronically means that more information may be kept for longer periods of time, if not indefinitely.\textsuperscript{92} Despite the differences in accessibility and retention of records, the federal government does not treat computerized records differently than paper records,\textsuperscript{93} and neither does Georgia.\textsuperscript{94}

E. RIGHT OF PRIVACY

The law recognizes the right of privacy in numerous areas, and there is some overlap between the different realms of privacy.\textsuperscript{95} There is a right of privacy in

---

\textsuperscript{90} See United States Dep't of Justice v. Tax Analysts, 492 U.S. 136, 156 (1989) (Blackmun, J., dissenting). Justice Blackmun stated:

\textbf{The result of [Tax Analysts's] now-successful effort in this litigation is to impose the cost of obtaining the court orders and opinions upon the Government and thus upon taxpayers generally. There is no question that this material is available elsewhere. But it is quicker and more convenient ... for respondent to have the Department do the work and search its files and produce the items than it is to apply to the respective court clerks.}

\textsuperscript{91} Id.

\textsuperscript{92} Solove, supra note 43, at 1154.

\textsuperscript{93} Freedom of Information Act, 5 U.S.C. § 552(a)(2)(D) ("Each agency, in accordance with published rules, shall make available for public inspection and copying ... copies of all records, regardless of form or format.").

\textsuperscript{94} Requests for computer generated information in light of the Open Records Act, 89 Op. Att'y Gen. (Ga.) No. 32, at 74 (1989) ("If public information not otherwise excluded or exempted is sought in a request and may be called up under an existing [computer] program, the Agency must comply.").

\textsuperscript{95} See Paul M. Schwartz, Property, Privacy, and Personal Data, 117 HARV. L. REV. 2055, 2058 (2004) ("Decisional and information privacy are not unrelated."); Solove, supra note 84, at 1431 ("Much of privacy law is interrelated.").
ELECTRONIC SIGNATURE EXCEPTION

F. INFORMATION PRIVACY

Information privacy in its fullest sense comes from neither the Constitution nor from tort law. Rather, information privacy, to the extent it exists, comes predominantly from statutes.

1. Constitutional Information Privacy: Whalen v. Roe and Progeny. Whalen v. Roe is generally considered the first Supreme Court case to acknowledge information privacy, though the Court did not use the phrase.\(^9\) Whalen announced that two interests are constitutionally protected, “the individual interest in avoiding disclosure of personal matters, and . . . the interest in independence in making certain kinds of important decisions.”\(^10\) The Court recognized information privacy in the form of an “interest in avoiding disclosure of personal matters” but found that the Constitution only imposes a duty to “avoid unreasonable disclosure.”\(^11\) The Supreme Court affirmed its Whalen decision in Nixon v. Administrator of General Services.\(^12\) The weakness in this constitutional right of privacy is that it can be outweighed by the public interest in disclosure.\(^13\)

---

96 Solove, supra note 43, at n.259, citing RESTATEMENT (SECOND) OF TORTS § 652A (1977) (“The privacy torts are often referred to collectively as ‘invasion of privacy’ and consist of (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light or ‘publicity’; and (4) appropriation.”); see also Solove, supra note 84, at 1432-34 (explaining how the existing privacy torts fail to provide appropriate information privacy).

97 Katz v. United States, 389 U.S. 347, 359 (1967) (“Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.”); see also id. at 350 (“[T]he Fourth Amendment cannot be translated into a general constitutional ‘right to privacy.’ That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further and often have nothing to do with privacy at all.”).


99 Whalen, 429 U.S. 589; Halstuk, supra note 62, at 79 (“Whalen remains the principal decision concerning constitutional protection of information privacy.”).

100 Whalen, 429 U.S. at 599-600.

101 Solove, supra note 84, at 1436; Whalen, 429 U.S. at 599-600.


103 Nixon, 433 U.S. at 457 (agreeing with the district court that the significant public interest in preserving the materials outweighed Nixon’s privacy interest, which was “quite small”); Whalen, 429 U.S. at 602-04 (rejecting appellee’s argument that “the knowledge that the information is readily available in a computerized file creates a genuine concern that causes some persons to decline needed medication” in light of the numerous disclosures required in healthcare, finding that the state has not deprived any individual of the right to decide independently to acquire and to use needed medication, and holding “that neither the immediate nor the threatened impact of the patient-
Related to the notion of information privacy is a right to anonymity. There is Supreme Court jurisprudence protecting anonymity, but that line of cases does not ensure information privacy. Since the 1977 cases of Whalen and Nixon, the Supreme Court has not ruled on information privacy as a constitutionally protected right.

2. **Statutory Protection of Information Privacy.** In contrast to the Supreme Court’s relative inactivity in this area, Congress has passed numerous statutes regarding the issue of privacy. With the Privacy Act of 1974, Congress indicated, among other things, that “the increasing use of computers and sophisticated information technology . . . has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information.” Since then, statutory protection of information privacy regarding private entities has come about on an ad hoc basis. In 1994, in response to state practices of selling information to private entities, Congress passed the Driver’s Privacy Protection Act (DPPA). The DPPA prohibits states from selling motor vehicle records. Professor Daniel Solove points out the importance of this legislation and gives examples of the large sums of money offered and paid to the states for motor vehicle information prior to the passage of the DPPA.

Identification requirements . . . on either the reputation or the independence of patients . . . is sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment”); see also Marc Rotenberg, *Restoring a Public Interest Vision of Law in the Age of the Internet*, 2004 DUKE L. & TECH. REV. 7 (“The U.S. Constitution doesn’t always provide the best material for privacy protection.”).


105 Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(2), 88 Stat. 1896; see also Solove, *supra* note 43, at 1172 (“The privacy protection that currently exists for public records is largely designed for a world of paper records and has been slow to adapt to an age where information can be downloaded from the Internet in an instant.”).

106 Stephen R. Bergerson, *E-Commerce Privacy and the Black Hole of Cyberspace*, 27 WM. MITCHELL L. REV. 1527, 1537 (“The existing federal statutes that protect consumer privacy from private intrusions are the result of a reactionary and piecemeal approach.”).


108 Id. § 2721. The statute states:

A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity: (1) personal information . . . about any individual obtained by the department in connection with a motor vehicle record [except for limited permissible uses or] (2) highly restricted personal information . . . about any individual obtained by the department in connection with a motor vehicle record, without the express consent of the person to whom such information applies, except [in limited circumstances].
of this federal law. Other federal privacy laws include Title V of the Gramm-Leach-Bliley Act, the Family Educational Rights and Privacy Act of 1974, the Fair Credit Reporting Act of 1970, and the Videotape Privacy Protection Act. Although the federal government has been the primary actor in the field of privacy, state legislatures have also created statutory privacy protections.

3. Technology Privacy Legislation. Privacy legislation exists also in the area of technology. In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) in order "to update and clarify federal privacy protections and standards in light of... new computer and telecommunications technologies. . . [including] electronic mail ("e-mail") [and] data transmission through computer networks." The subsequent passage of the Children's Online Privacy Protection Act in 1998 reveals Congress's concern for the negative effects of information collection by website operators and online services on children.

---

109 Solove, supra note 43, at 1150. Solove notes: For decades, many states have been selling their public records to the highest bidder. Colorado used to sell its motor vehicle information for about $4.4 million a year. Florida offered to sell copies of its motor vehicle information for $33 million. New York earned $17 million in one year from such sales.


Congress has not been the only legislative body to enact technology privacy legislation. In 2001, New York, confronting the issue of privacy in the information age, enacted its Internet Security and Privacy Act.117

4. Information Privacy at its Fullest. Professor Jerry Kang uses the Information Infrastructure Task Force's definition of information privacy, stating that: "Information privacy is 'an individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used.'"118 At the heart of this definition is the phrase "personal information."119 In the definition, the term "personal" refers to the notion that the information is traceable to an individual.120

Kang describes three ways in which information can be traceable to an individual. First, information may have an authorship relation.121 Second, information can bear "a descriptive relation."122 Third, information may be identifiable in the form of an artificial "mapping relation."123 The first category includes information authored by the individual such as an e-mail or letter.124 Information with a descriptive relationship includes information that is biological,125 biographical,126 or social127 in nature as well as information about the activities of an individual such as the details of a purchase or visit to a website.128 Information not bearing an authorship or descriptive relationship may be personal in the sense of information privacy if it is linked to the individual "for institutional identification, secured access, or provision of some service or good."129 Typically, mapping information is in no way related to the individual outside the institutional system.130 Examples of mapping information include social security numbers, network passwords, and personal identification numbers (PINs) for automatic teller machines.131 Components of a digital signature, to the

119 Kang, supra note 118, at 1206.
120 Id. at 1206-07.
121 Id. at 1207.
122 Id.
123 Id.
124 Id.
125 For example, height, weight, blood type.
126 For example, birth date, sexual orientation, criminal history.
127 For example, membership in religious and political groups.
128 Kang, supra note 118, at 1207.
129 Id. at 1207-08.
130 Id. at 1208.
131 Id.
extent those components are like passwords, and some electronic signature information would fall within this category. Some information may fall into multiple categories; for example, the use of a mother’s maiden name as a password is both an instrumentally mapped and a descriptive piece of information.132

In order to understand the meaning of the term “personal information” fully, it is helpful to understand the concept of nonpersonal information. Nonpersonal information is not traceable to an individual, and thus not private under the definition of information privacy.133 Three categories of nonpersonal information exist: information that is not about a human being, anonymous information that may not be linked to a specific individual, and information directly identifiable to a group but only indirectly identifiable to an individual within that group.134 One example of clearly nonpersonal information in this third category is a stock price for a large corporation.135

The courts have not clearly recognized information privacy defined as such. Instead, the case law reveals a tendency of courts to apply what Professor Solove calls “the secrecy paradigm,” a conception that privacy is not protected after information has been disclosed.136 Application of the secrecy paradigm is inadequate, however, because of the threat of databases “to freedom in general . . . that implicates the type of society we are becoming, the way we think, our place in the larger social order, and our ability to exercise meaningful control over our lives.”137 Professor Solove argues that the fear of surveillance and “Big Brother” is misdirected in the context of databases and information storage by the government and private entities in part because much of our personal information, including financial information, gender, race, marital status, and occupation, is not embarrassing.138 Instead of Orwell’s 1984 Big Brother model, Solove would use Kafka’s The Trial as the model to which drafters of privacy policy should eschew.139 Databases pose a threat because of the manner in which bureaucratic processes treat individuals and their information.140 Through bureaucratic processes, government officials collect and disseminate personal information

132 Id.
133 Id.
134 Id. at 1208-10.
135 Id. at 1210.
136 Solove, supra note 43, at 1176-84.
137 Id. at 1177 (“In the Information Age, this paradigm is outmoded, and it could lead to the practical extinction of privacy.”).
138 Solove, supra note 84, at 1418-19.
139 Id. at 1418-26.
140 Id.
141 Id. at 1422.
without using discretion. In this system, no individual is permitted to make
decisions about his information.\textsuperscript{142} For example, state and federal open records
laws require state agencies to release information without regard to how it may
affect an individual.\textsuperscript{143} Databases, as well as the manner in which information
contained in them is used, effectively disempower individuals by removing any
control these individuals have over their personal information.\textsuperscript{144}

A more effective privacy regime would provide individuals with some control
over information that potentially affects employment, professional licensure, and
credit.\textsuperscript{145} Privacy should also allow individuals to correct errors or expunge data
in government databases.\textsuperscript{146} Insofar as information privacy, as defined above,
departs from what Solove terms “the secrecy paradigm,”\textsuperscript{147} it is an important step
in addressing the real problems with information in databases.

G. THE INCREASING NEED FOR PRIVACY LEGISLATION

1. The Need for Legislation Generally. Public records and the information in
them were once relatively inaccessible.\textsuperscript{148} Even with a growing government
bureaucracy—meaning more information in the hands of the government—and
open records laws, until very recently there was a reasonable expectation of
privacy “not in the sense that the information [would] be completely shielded
from public access, but in the sense that for the most part, it [would] be lost in a
sea of information about millions of people.”\textsuperscript{149} As public access increased, that
expectation was no longer well founded.\textsuperscript{150} As Professor Lillian BeVier points

\textsuperscript{142} Id. ("Bureaucratic decisionmaking processes are being exercised ever more frequently over a
greater sphere of our lives, and we have little power or say within such a system, which tends to
structure our participation along standardized ways that fail to enable us to achieve our goals, wants,
and needs.").

\textsuperscript{143} See, e.g., Freedom of Information Act, 5 U.S.C. § 552; FLA. STAT. ANN. § 119; O.C.G.A. § 50-
18-72.

\textsuperscript{144} Solove, supra note 84, at 1423. The facts contained in databases “fail to tell the entire story”
but important decisions are made based on those limited facts. \textit{Id.} at 1424.

\textsuperscript{145} \textit{Id.} at 1426.

\textsuperscript{146} \textit{Id.}

\textsuperscript{147} Solove, supra note 43, at 1176-84 (discussing the “secrecy paradigm” and related cases).

\textsuperscript{148} \textit{Id.} at 1178.

\textsuperscript{149} \textit{Id.}

\textsuperscript{150} \textit{Id.;} Amy Harmon, \textit{As Public Records Go Online, Some Say They're Too Public}, N.Y. TIMES, Aug.
24, 2001, at A1 (quoting Deirdre Mulligan, director of the Law, Technology and Public Policy Clinic
at the University of California at Berkeley law school). Harmon states:
At the time many of the public records laws on the books came about there was
no need to build privacy safeguards in because there was no threat . . . [n]ow
people are being forced to say those government records contain some
exceedingly detailed information about people's personal lives, and the cost of
out, even prior to computers "information was difficult to protect from 
unwarranted disclosure" because information is easily stolen and thefts are seldom 
detected since victims rarely know that anything has been lost.\textsuperscript{151} BeVier discusses 
two features of technology that explain why computer technology has exacerbated 
the problem.\textsuperscript{152} First, computers allow for the efficient compilation and 
comparison of data.\textsuperscript{153} This means that the information that was "lost in a sea of 
information"\textsuperscript{154} before can be quickly searched and reorganized to fit the user's 
needs. The benefits of this efficiency are obvious. For example, "computer 
profiling, which searches for specified elements or combinations of elements in 
a number of different record systems," can help identify possible tax evaders and 
narcotics dealers.\textsuperscript{155} On the other hand, there are negative effects. For instance, 
the other side of profiling is that government officials may "go on 'fishing 
expeditions' rather than targeting their investigations to people reasonably 
suspected of crime" or use information in racially or otherwise biased ways.\textsuperscript{156} 
Second, new technology disseminates government control of information.\textsuperscript{157} 
Computer records systems are linked via telecommunications systems, which 
results in both more information being exchanged and more people accessing that 
information.\textsuperscript{158} The United States Department of Justice Office of Information 
Privacy wrote in 1990 that "no development in the history of the [FOIA] has held 
as much potential for shaping its contours, even the very future of its implement-
tation, as that of new technology."\textsuperscript{159}

2. \textit{Examples of the Misuse of Information Obtained Through Open Records Laws.} In 
1998, \textit{Dateline} detailed the story of one woman who has lived in fear since she

\begin{itemize}
\item[\textsuperscript{151}] BeVier, supra note 82, at 472.
\item[\textsuperscript{152}] Id.
\item[\textsuperscript{153}] Id. at 473 (referring to this feature with the term "multifunctionality"); Schwartz, supra note 61, at 587 (describing the term "data matching," defined as "the electronic comparison of two or more sets of records in order to find individuals included in more than one data base," as a process that clearly makes compilation of information easier).
\item[\textsuperscript{154}] See supra text accompanying note 149.
\item[\textsuperscript{155}] BeVier, supra note 82, at 473.
\item[\textsuperscript{156}] Id.
\item[\textsuperscript{157}] Id. at 474; see also Schwartz, supra note 61, at 587-88 ("The federal government now carries out data matching on billions of records. One survey of only a small portion of federal matching programs identified data exchanges in one five-year period involving seven billion records. Single matches have been carried out on as many as fifteen million records.").
\item[\textsuperscript{158}] BeVier, supra note 82, at 474.
\item[\textsuperscript{159}] Cate et al., supra note 6, at 66 (quoting Office of Information and Privacy, Department of Justice, Department of Justice Report on "Electronic Record" FOIA Issues 3 (1990); see also id. at 67 ("[A]pplying the FOIA to electronic agency records exacerbates the significant invasion of personal privacy and intrusion into organizational decision-making occasioned by requesting information having nothing to do with government activities.").
\end{itemize}
learned that her ex-boyfriend, imprisoned for murder, obtained her address under a state FOIA. Even more chilling is the tragedy of Amy Boyer. In 1999, a high school classmate of Boyer, Liam Youens, "who had been obsessed with Boyer since junior high school, paid Docusearch Inc. . . . about $150 for Boyer’s Social Security number and other information, including her work address." After obtaining the information, Youens shot and killed Boyer as she left work. Although Youens did not obtain the information directly from a government agency, "information brokers . . . compile public records from different government entities and corporations throughout the U.S. to develop databases, from which [these information brokers] pull information.”

H. OPEN RECORDS LAW: ELECTRONIC SIGNATURE EXCEPTIONS

Georgia law excepts from public disclosure “[p]ublic records containing information that would disclose or might lead to the disclosure of any component in the process used to execute or adopt an electronic signature, if such disclosure would or might cause the electronic signature to cease being under the sole control of the person using it.” Similarly, Ohio, within its UETA, removes “[r]ecords that would disclose or may lead to the disclosure of records or information that would jeopardize the state’s continued use or security of any computer or telecommunications devices or services associated with electronic signatures, electronic records, or electronic transactions” from public records subject to disclosure.

III. DISCUSSION

States approach the unique problem posed by the interaction of privacy law, open records law, technology-neutral electronic signature law, and rapidly changing technology differently. The Georgia Legislature seems to have used an


The prisoner . . . claimed that he was the father of her child and needed the address because he wanted to file a paternity suit. This story illustrates why it is important for people to be able to obtain certain information about others, yet also demonstrates the dangers and threat to privacy caused by the ready availability of information.

161 Barnes, supra note 86.
162 Id.
163 Id.
165 OHIO REV. CODE ANN. § 1306.23 (Supp. 2004).
imperfect approach, inadvertently creating a broad exception to its open records law. The current law fails to reflect the policies typical of Georgia open records law and creates an unintended privacy exception. Although the Georgia Legislature effectively produced technology-neutral electronic signature legislation, it likely created a larger privacy exception than intended.

A. THE HISTORY OF CHANGES IN THE GEORGIA LAW AND HOW THE BROAD EXCEPTION WAS CREATED

In 1996, the Georgia Digital Signature Task Force (Digital Task Force) drafted a digital signature bill patterned after the Utah digital signature statute. The legislature considered the bill in the 1996 legislative session but the bill was tabled. The Digital Task Force drafted a different, simpler bill, Senate Bill 103, patterned after Florida’s Electronic Signature Act of 1996. Senate Bill 103 not only defined the term “electronic signature” but also added the electronic signature exception to the Open Records Statue. Georgia did not define the term “electronic signature” broadly as Florida had; rather, Senate Bill 103 confined the definition of electronic signature to those methods having the qualities of a digital signature. As the law existed from 1997 to 1999, the electronic signature exception was not overly broad and posed no real threat to transparency. Then, in 1999, Georgia amended the Georgia Electronic Records and Signatures Act to change the definitions. According to one commentator, the legislature made this change in response to “the issue of evolving electronic

167 Id.
168 Id.; see also text accompanying note 26.
169 Johnson, supra note 166, at 26; see also 1997 Ga. Laws 1052, §§ 1, 2 (codifying Senate Bill 103).
170 See Act effective May 25, 1996, 1996 Fla. Laws ch. 96-224 at 838 (defining digital signature first, then defining electronic signature to encompass more than digital signatures).
171 See Act of Apr. 22, 1997, 1997 Ga. Laws 1052, 1053, which states: ‘Electronic signature’ means an electronic or digital method executed or adopted by a party with the intent to be bound by or to authenticate a record, which is unique to the person using it, is capable of verification, is under the sole control of the person using it, and is linked to data in such a manner that if the data are changed the electronic signature is invalidated.
transactions" and the proposal of a member of the Georgia Electronic Commerce
Association. The amendment redefined electronic signature very broadly and
created a new term, "secure electronic signature," which followed the exact
language previously used to define electronic signature. This amendment
created a flaw in Georgia law because, while the definitions had been amended,
the legislature failed to modify the exception to the open records statute to
parallel those changes in the definitions of terms.

B. WHEN ELECTRONIC SIGNATURE LEGISLATION MEETS OPEN RECORDS LAWS

The Georgia Legislature may have inadvertently created just the kind of
exception proponents of privacy would have drafted. By using general, overly
broad statutory language in order to become technology-neutral, the legislature
created a loophole in the open records law that agencies can use to withhold
documents that would have necessarily been disclosed under the law prior to
1999. The statutory language "would disclose or might lead to the disclosure
of" allows for considerable discretion. Furthermore, the definition of the term
"electronic signature" is given such a broad definition that essentially any record
containing personally identifiable information may be lawfully withheld from
public disclosure.

In 1990, the Georgia Supreme Court decided the case of Dooley v. Davidson,
which arose out of a dispute over whether certain records were subject to
disclosure under the Open Records Act. Examining the records at issue in the
Dooley case is illustrative of the broad privacy implications of Georgia’s current
law.

175 The Georgia open records statute states, "For purposes of this paragraph, the term 'electronic
signature' has the same meaning as that term is defined in Code Section 10-12-3." O.C.G.A. § 50-
176 See supra Parts II.B and III.A.
178 Georgia defines "electronic signature" as "a signature created, transmitted, received, or stored
by electronic means." O.C.G.A. § 10-12-3(3) (2000). Within that definition, the definitions of
"electronic" and "signature" expand the breadth of what is included in a Georgia "electronic
signature." See O.C.G.A. § 10-12-3(1) (" 'Electronic' means, without limitation, analog, digital,
electronic, magnetic, mechanical, optical, chemical, electromagnetic, electromechanical, electrochemical,
or other similar means."); O.C.G.A. § 10-12-3(7) (" 'Signature' means any symbol or method that
a person causes to be attached to or logically associated with a record with the intent to sign such
record.").
179 397 S.E.2d 922, 923 (Ga. 1990).
In *Dooley*, two newspapers requested records concerning the income, including income from sources outside the University, of all University of Georgia coaches.\(^{180}\) The coaches produced thirteen documents in response to discovery motions.\(^{181}\) Documents One, Two, and Three were reports prepared by the coaches concerning outside income.\(^{182}\) Document Four was a contract obligating a coach to make speaking appearances on behalf of a manufacturer.\(^{183}\) Documents Five, Six, Seven, Ten, and Thirteen were contracts between coaches and suppliers of sports equipment and apparel.\(^{184}\) Documents Eight and Nine were letters relating to compensation for participation in radio programs.\(^{185}\) Document Eleven contained financial information regarding promotional radio and television broadcasts.\(^{186}\) Document Twelve was a contract with the producer of a radio network obligating a coach to provide commentary during the broadcast of select basketball games.\(^{187}\)

At issue in the case was whether the records before the court were public records under Georgia law.\(^{188}\) For reasons not relevant to this Note, the court found that ten of the thirteen documents were public records subject to disclosure under the law.\(^{189}\) Seven of the thirteen documents were contracts.\(^{190}\) Of those seven, the court determined only the five contracts between the sports equipment and apparel suppliers were public records under title 50, section 72(a) of the Georgia Code.\(^{191}\) The court found the two letters, Documents Eight and Nine, to be public records subject to disclosure under the law.\(^{192}\) Under the current law,
while the same five contracts and the two letters are still public records, the electronic signature exception would likely apply to except each of these documents from disclosure.

Presumably, at least one person signed each of the contracts and the two letters. The physical signatures on the documents place the contracts within the electronic signature exception. The signature on the letter or contract (or a signature on a memorandum, letter, or check) "would disclose or might lead to the disclosure of any component in the process used to execute or adopt an electronic signature," because the possessor of that written signature could scan the document into an image-based file, such as a .pdf file, and the act of converting the writing into an electronic format would make that file a component of "a signature stored by electronic means," and thus, an electronic signature under the current law. This example reveals that no document with any individual's signature on it would be subject to disclosure. Thus, no document signed by the governor or an agency official would fall outside the exception, and the open records law would fail in its purpose.

Assuming that the reports prepared by the coaches (Documents One, Two, and Three) were not physically signed, the same analysis could not stand. Nonetheless, the electronic signature exception may apply. The mere existence of a name on the piece of paper is arguably a "component in the process used to execute or adopt an electronic signature." This is so because even a typed name at the bottom of an e-mail can serve as an electronic signature; thus, possession of the coaches' names could be sufficient to qualify. The court would likely reject this argument as nonsensical since a name is easily obtained, particularly when it is a college coach's name and no harm could be done by the release of the name. If the court considered the fact that the additional information in the document might enable someone to produce a more convincing e-mail message, however, then the argument for nondisclosure might hold up in court. This is, of course,

---

193 Because the relevant statute has been modified only slightly and the Georgia supreme court has not overruled Dooley, there is no reason to believe that a Georgia court would find the five contracts or two letters not public records.


195 See id. (evaluating contracts).


197 O.C.G.A. § 10-12-3(3) ("Electronic signature" means a signature created, transmitted, received, or stored by electronic means and includes but is not limited to a secure electronic signature.").

198 Id.


200 See supra note 18.
more of a security issue than a privacy issue, but the language of the statute does not necessarily foreclose such arguments.

The final document released in the Dooley case was Document Eleven, which "concerns financial information relative to radio and television broadcasts." If the name argument described above were unavailable for this document—that is, if the financial information provided no name—a reasonable argument against disclosure would probably not exist. If no personal information, such as a social security number, bank account number, or name, was in the document and it consisted solely of numbers, the electronic signature exception would probably not exempt the document from disclosure.

In sum, the facts of the Dooley case applied under current law demonstrate the potentially sweeping effects of the electronic signature exception. In the actual case, eleven documents were released. Under the current law, it is likely that, at most, only four of the documents would be subject to disclosure. Similarly, a large number of government documents that were formerly subject to disclosure are now exempt under the electronic signature exception.

C. THE PROBLEM OF USING THE EXCEPTION

Even though Georgia now has a very broad exception to disclosure, the full implications of the exception may never be realized. First, because most people will never know that records containing their personal information are being released, there may be little opportunity for challenge. The only people who might deploy the exception to prevent the release of records are those working for agencies or their attorneys. In most instances, the agency would prefer to disclose a record over withholding a record and incurring court costs. Only when entities subject to public records laws fear fraud are they likely to aggressively argue the electronic signature exception. One example might be a university which is asked to disclose checks to a requester. Fearing fraud, a university might search for a reason not to disclose the record and find that the electronic signature exception is the only available argument for nondisclosure. It is possible that an individual could learn of a potential disclosure, as the coaches in the Dooley case did, and argue that the statue mandates nondisclosure. Outside such a situation, however, there is little chance of the exception being deployed.

---

201 See Dooley, 397 S.E.2d at 926.
202 See O.C.G.A. § 50-18-72(h) (providing that "the public officer or agency having control of such record or records, if access to such record or records is denied in whole or in part, shall specify in writing the specific legal authority exempting such record or records from disclosure, by Code section, subsection, and paragraph").
Second, the law expressly provides that title 50, chapter 18, section 72 of the Georgia Code "shall be interpreted narrowly."\(^{203}\) Taking this language in conjunction with the purpose of the open records law, it is possible that courts would reject arguments for nondisclosure based on the electronic signature exception. Still, the plain language of the statute is very broad, and even a narrow interpretation of the terms "may" and "might lead to" gives the exception broad reach.

D. PROPOSAL FOR AMENDMENT

The simplest and best solution, and one that comports with the general intent of the open records statute, is to restrict the amount of information within the exception. The exception would be far less expansive if the phrase "electronic signature" were changed to "secure electronic signature" as defined by the same statutory section.\(^ {204}\) This change would make the law more logical and serve to close the current loophole. In terms of logic, it makes sense to keep all the components of a secure electronic signature "under the sole control of the person using it."\(^ {205}\) On the other hand, from a security standpoint, it makes no sense for the components of an electronic signature to be under the sole control of the person using it simply because electronic signature has such a broad definition. The Georgia Legislature likely either did not understand or did not consider the implications of this exception. The history of the open records electronic signature exception and the electronic signature law seems to indicate that the legislature overlooked the reference to the definitional portion of the electronic signature statute contained in title 50, chapter 18, section 72(a)(12) when the legislature amended the electronic signature law.\(^ {206}\)

IV. CONCLUSION

Advances in technology facilitating electronic commerce and the attempts to shape the law to foster electronic commerce rather than restrict it have resulted in technology-neutral electronic signature legislation. This effort to encourage electronic commerce has created ripples in other fields of the law. One such field is government record keeping and public access to those records. Public access to government records is a mainstay of the federal and state governments under the rationale that the press and the public will serve as watchdogs over the

\(^{203}\) O.C.G.A. § 50-18-72(g).

\(^{204}\) O.C.G.A. § 10-12-3.

\(^{205}\) Id.

\(^{206}\) See infra Part III.A.
government. Information privacy is also intertwined in the field of government records and public access to those records. Information privacy concerns extend even beyond government records into the arena of privately held documents—particularly those held by businesses engaged in marketing efforts or selling information to other businesses or individuals.

In adapting its law to facilitate electronic commerce, the Georgia Legislature has upset the prior balance of privacy and open records in the state and created an overly broad exception to the general requirement of disclosure of government records. Georgia should amend its open records law in order to revert to a state with a generous policy for the disclosure of government records even though it does create a potential source of privacy protection. The history of the Georgia Electronic Records and Signatures Act seems to indicate that the exception was created inadvertently. Privacy could be better protected with intentional legislation aimed at providing information privacy. The simple addition of the word "secure" to the open records electronic signature exception will close the current loophole, and the Georgia Legislature should therefore adopt this addition.

MICHAEL L. VAN CISE