E-mail

Privacy and Public Records in Florida

By:
Matthew M. Henry

For:
Ben F. Overton, Senior Justice of the Florida Supreme Court
Florida Constitutional Law & The Florida Supreme Court Seminar
University of Florida

April 23, 2004

I. Introduction

An individual's privacy in electronic mail, or e-mail, has been relatively undefined until recent years. The common law constitutional right of privacy and Florida's express right of privacy apply to personal e-mail of private employees and employees of state and local government entities in different ways. The public has substantial access government information, but the private employer may be less restricted in what information it takes from its employees. Because established laws are being applied to new advances in technology, the courts have had to clarify how e-mail is to be treated in relation to public records provisions and in respect to discovery of e-mail in civil or criminal proceedings.[1]

[1] "Our rapidly expanding digital world has created many opportunities for immediate public access to government records and governmental activities. At the same time, it has made accessible some types of information that blur the lines between public and private information. There is little question that our policies and procedures surrounding public records, and perhaps our entire concept of public records, need constant review to maintain a proper balance between the public's right to know about the operation of its democratic government and other competing interests." Times Publ'g Co. v. City of Clearwater, 830 So. 2d 844, 848 (Fla. 2d DCA 2002).

II. The Florida Constitution on Privacy and Public Records

A. Privacy under the Florida Constitution

Florida is the first state to provide an express right to privacy in its constitution[2], and it is still one of the few that has yet to do so[3]. The explicit right of privacy was added by voters to the Constitution of the State of Florida in 1980,[4] two years after the proposal had been suggested to the Constitutional Revision Commission by then Chief Justice for the Florida Supreme Court, Ben F. Overton.[5] Article I, section 23 of the Florida Constitution states:

> § 23. Right of privacy
>
> Every natural person has the right to be let alone and free from governmental intrusion into

---

[2] Fla. Const. Art. I, § 23 (2004).

[3] The Honorable Ben F. Overton & Katherine E. Giddings, *Article: The Right to 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, 26 (1997).
In addition to Florida, Alaska, Arizona, California, Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington have right of privacy provisions in their state constitutions. *See generally* Cope, *To Be Let Alone: Florida's Proposed Right of Privacy*, 6 Fla. St. U.L. Rev. 673 (1978).

[4] *Id.*

[5] *Id.* at 34.

> 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.[6]

This express provision grants more protection than the implied federal right of privacy because it extends to all aspects of an individual's private life rather than an interpreted penumbra of rights.[7] Article I, section 23 protects from governmental intrusion into one's private life absent a compelling state interest.[8] "Every natural person" has been interpreted to encompass all Floridians, including minors.[9]

However, the reach of this constitutional provision does have limitations. It does not protect against private or commercial intrusion.[10] Similarly, an individual's public life is not secured by the language of this constitutional provision.[11] Additionally, exception to the protection of this express right is made for the public's

---

[6] Fla. Const. art. I, § 23.

[7] 25 Fla. St. U.L. Rev. 25 at 40.

[8] *Id.* at 35, 40-41.

[9] *Id.* at 35.

[10] *Id.* at 41.

[11] *Id.* at 35.

right of access to public records and meetings as provided by law.[12]

B. Public Records under the Florida Constitution

Florida has taken pride in its policy of open-door government.[13] Under what is known as Sunshine Laws,[14] statutes had already secured public access to meetings and records of state and local government entities. Access to public records and meetings became elevated to a right provided by the state constitution in 1992,[15] as concerns crew that the rights of access might be carved away or diminished by ordinary legislative action[16] and as media became concerned that legislative meetings might be closed to the public.[17] Article I, section 24 of the Florida Constitution solidifies a public right of access to public records with the following language:

> § 24. Access to public records and meetings
>
> (a) Every person has the right to inspect or copy any public record made or received in connection with the official business of any public body, officer, or employee of the state, or persons acting on their behalf, except with respect to

---

[12] *Id.* at 36-37; Fla. Const. art. I, § 23.

[13] Florida Attorney General Charlie Crist, *Florida's Government-in-the-Sunshine Law*, (2004), at http://myfloridalegal.com/sunshine; 25 Fla. St. U.L. Rev. 25 at 53.

[14] *Id.*; Fla. Stat. ch. § 286.

[15] Fla. Const. art. I, § 23.

[16] Lecture by Ben F. Overton, Senior Justice, Florida Supreme Court, in Gainesville, Fla. (Apr. 9, 2004).

[17] Florida Attorney General Charlie Crist, *Florida's Government-in-the-Sunshine Law*, (2004), http://myfloridalegal.com/sunshine.

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, and districts; and each constitutional officer, board, and commission, or entity created pursuant to law or this Constitution.

[Part b, pertaining to public meetings has been omitted].

(c) This section shall be self-executing. The legislature, however, may provide by general law passed by a two-thirds vote of each house for the exemption of records from the requirements of subsection (a) and the exemption of meetings from the requirements of subsection (b), provided that such law shall state with specificity the public necessity justifying the exemption and shall be no broader than necessary to accomplish the stated purpose of the law. The legislature shall enact laws governing the enforcement of this section, including the maintenance, control, destruction, disposal, and disposition of records made public by this section, except that each house of the legislature may adopt rules governing the enforcement of this section in relation to records of the legislative branch. Laws enacted pursuant to this subsection shall contain only exemptions from the requirements of subsections (a) or (b) and provisions governing the enforcement of this section, and shall relate to one subject.

(d) All laws that are in effect on July 1, 1993 that limit public access to records or meetings shall remain in force, and such laws apply to records of the legislative and judicial branches, until they are repealed. Rules of court that are in effect on the date of adoption of this section that limit access to records shall remain in effect until they are repealed.[18]

[18] Fla. Const. art. I, § 24.

The public records provision provides a right to inspect or copy records made or received in connection with the official business of any public entity of the state.[19] However, the section also allows the legislature to make exemptions by a two-thirds vote of both houses,[20] which is higher than the simple majority that would have otherwise been required under normal legislation. Further, the statute creating such an exemption both (1) "shall state with specificity the public necessity justifying the exemption" and (2) "shall be no broader than necessary to accomplish the stated purpose of the law."[21] Additionally, other guidelines under the Florida Constitution must be complied with, including a single-subject legislation requirement.[22] With such stringent protections defined in the state's governing doctrine, the constitutional right to access public records is much stronger than it was when it was only secured by ordinary statute. Plus, the constitutional provision works in conjunction with statutes, because the legislature is granted the power to

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Fla. Const. art. III, § 6.

control the process by which public records are made accessible, maintained, and destroyed.[23]

This 1992 constitutional amendment also addressed the access to public records of the courts.[24] The judiciary had adopted its own rule regulating the availability of public records, the exemptions to disclosure, and the disposal of records.[25] The amendment sought to fix, on July 1, 1993, the rules at the status quo while resolving any separation of powers conflicts that might arise from the legislature having the authority, or the ability to delegate authority, to regulate all public records, including those of the judiciary. The Florida Supreme Court quickly updated their rules upon learning that they would be fixed once the amendment took effect.[26] The Florida Supreme Court still independently sets perimeters for access to, maintenance of, and destruction of administrative and court documents that might be public records through Rules of Judicial Administration.[27] It further educates employees on these

---

[23] Fla. Const. art. I, § 24; *See* Fla. Stat. ch. 119 (2004).

[24] Fla. Const. art. I, § 24.

[25] Lecture by Ben F. Overton, Senior Justice, Florida Supreme Court, in Gainesville, Fla. (Feb. 27, 2004).

[26] *Id.*

[27] Rule 2.051 "Public Access to Judicial Branch Records,"

responsibilities in handbooks and other materials on policy.[28] The courts make it clear that electronic records are to be treated the same as paper records, in that distinctions or based on the subject matter of the record rather than the form.[29]

Rule 2.075 "Retention of Court Records," Rule 2.076 "Retention of Judicial Branch Administrative Records," and "State of Florida Judicial Branch Records Retention Schedule for Administrative Records." Florida Rules of Judicial Administration: 2004 Edition, at http://www.flabar.org/TFB/TFBResources.nsf/Attachments/63413B851B738BA585256B29004BF86B/$FILE/04judadm.pdf?OpenElement.

[28] "Generally, all Court records are open to public inspection except the work product of the justices and their staffs, vote and remark sheets placed in individual case files, justice assignment records maintained by the clerk's office, portions of case records sealed by a lower court, case files which are confidential under the rules of the Court, and internal case management data. Access to the Court's public records is governed by Florida Rule of Judicial Administration 2.051." Manual of Internal Operating Procedures § I(D): Updated January 2002, at http://www.flcourts.org/pubinfo/documents/IOPs.pdf.

[29] In re Amendments to Rule of Judicial Admin. 2.051 - Pub. Access to Judicial Records, 651 So. 2d 1185, 1186-1187 (Fla. 1995). *See* "State of Florida Judicial Branch Records Retention Schedule for Administrative Records." Florida Rules of Judicial Administration: 2004 Edition, at http://www.flabar.org/TFB/TFBResources.nsf/Attachments/63413B851B738BA585256B29004BF86B/$FILE/04judadm.pdf?OpenElement.

III. Florida Statutes on Public Records

The Florida Statutes largely delegates the responsibility of making public records accessible to its individual agencies and subdivisions. The legislature requires that a policy be established, giving notice of how the agency will handle various details such as records requests,[30] fees,[31] document disposal.[32] Each agency is supposed to designate who will determine whether the document is a public record and maintain those designated as such.[33] Lawmakers were clear in providing that, while they encourage the increased usage of electronic records, the right to access public records should in no way be displaced by the use of a new medium,[34] as can be seen in the language of section 119.01 and the broad definition of public records in section 119.011:

> § 119.01. General state policy on public records
>
> (1) It is the policy of this state that *all* state, county, and municipal *records shall be open* for personal inspection by any person.
>
> (2) The Legislature finds that, *given*

[30] Fla. Stat. §§ 119.06, 119.07 (2004).

[31] Fla. Stat. § 119.07 (2004).

[32] Fla. Stat. § 119.041 (2004).

[33] Fla. Stat. § 119.021 (2004).

[34] Fla. Stat. §§ 119.01(2), 119.01(3) (2004).

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. If an agency provides access to public records by remote electronic means, then such access should be provided in the *most cost-effective and efficient manner* available to the agency providing the information.

(3) The Legislature finds that providing access to public records is a duty of each agency 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*.

(4) *Each agency shall establish a program for the disposal of records* that do not have sufficient legal, fiscal, administrative, or archival value in accordance with retention schedules established by the records and information management program of the Division of Library and Information Services of the Department of State.[35]

§ 119.011. Definitions

For the purpose of this chapter:

(1) "Public records" means *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*.

(2) "Agency" means any state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or

[35] Fla. Stat. § 119.01 (2004) (emphasis added).

> established by law including, for the purposes of this chapter, the Commission on Ethics, the Public Service Commission, and the Office of Public Counsel, and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency.[36]

IV. Case Law: *City of Clearwater*

In *State v. City of Clearwater*,[37] the Supreme Court of Florida, in answering a rephrased certified question of great public importance from the Second District Court of Appeal, addressed how to deal with e-mail in the setting of public records law.[38] While the case can appear at first glance to be a victory for privacy rights advocates, the decision only pertains to public records since no privacy rights were asserted by the parties.[39] The Florida Supreme Court reiterated important factors that the Second District stressed were not at issue in this case. The case did not address (1) "e-mails that may have been isolated by a government employee whose job required him or her to locate employee misuse of government computers"; (2) "a balancing

---

[36] Fla. Stat. § 119.011 (2004) (emphasis added).

[37] State v. City of Clearwater, 863 So.2d 149 (Fla. 2003).

[38] *Id.* at 150.

[39] *Id.* at 154; Times Publ'g Co. v. City of Clearwater, 830 So. 2d 844, 845-846 (Fla. 2d DCA 2002).

of the public's interest in open public records and an individual's right to privacy"; or (3) "an in camera inspection of records."[40]

In the facts of that case, "a Times Publishing Company reporter requested that the City of Clearwater provide copies of all e-mails either sent from or received by two city employees over the City's computer network" over the course of about a year.[41] The Times was not satisfied when the City turned over only public e-mails, after the employees had separated public and private e-mails pursuant to City procedures.[42]

The Times contended that the generation and storage of e-mails on government-owned computers dictated that the e-mails were public records by that placement, "regardless of their content or intended purpose."[43] The State of Florida contended that "the headers created by e-mails when they

---

[40] *Id.* at 151 n.2, (*citing* Times Publ'g Co. v. City of Clearwater, 830 So. 2d 844, 845-846 (Fla. 2d DCA 2002)).

[41] State v. City of Clearwater, 863 So.2d 149, 150 (Fla. 2003).

[42] *Id.* at 150-151.

[43] *Id.* at 151.

are sent are akin to phone records or mail logs, which the State asserts are clearly public records."[44]

The Florida Supreme Court found both arguments without merit and upheld the Second District Court's decision.[45] "'Personal' e-mails are not 'made or received pursuant to law or ordinance or in connection with the transaction of official business' and, therefore, do not fall within the definition of public records in section 119.011(1) by virtue of their placement on a government-owned computer system."[46] For e-mails to be public records, "the e-mails must have been prepared 'in connection with the official agency business' and be 'intended to perpetuate, communicate, or formalize knowledge of some type.'"[47] The Court reasoned that "[t]he determining factor is the nature of the record, not its physical location."[48] It did so by analogizing to various practical situations including such circumstances where a government-owned post-office box was used to deliver a personal letter or bill that is kept in a

---

[44] *Id.*

[45] *Id.*

[46] *Id.* at 155.

[47] *Id.* at 154.

[48] *Id.*

government-owned desk or filing cabinet, and yet obviously is not to be considered a public record.[49] In essence, the Florida Supreme Court looked at its own policies and procedures and applied the same standard to this case, in respect to determining what e-mail records to make publicly available in a manner similar to a letter or memo and in respect to maintaining the e-mail records within technologically feasible limits.[50]

---

[49] *Id*. at 153, 154.

[50] "We conclude that the supreme court, each district court of appeal, and each judicial circuit should establish, when e-mail is implemented in their particular jurisdiction, transmission systems that allow officials and employees the means to manually store official business transaction e-mail that is non-exempt either electronically or on hard copy. The protocol for maintaining non-exempt e-mail records that relate to the transaction of official business by any court or court agency should be developed by each judicial entity consistent with the technology available in its jurisdiction. While we do not believe that the constitution requires that we electronically archive all e-mail messages sent or received, we do emphasize that all judicial officials and employees are obligated to ensure that non-exempt official business e-mail records are not lost. One way of satisfying this obligation is for judicial officials and employees to have an electronic means to store non-exempt official business e-mail transmissions. An alternative is to make a hard copy of any e-mail transmission related to the transaction of official business by any court or court agency and to file the copy appropriately. These approaches are no different from the present obligation on judicial officials and employees who receive or send communications in connection with the transaction of official business, be it by memo or letter." In re Amendments to Rule of Judicial Admin. 2.051 - Pub. Access to Judicial Records, 651 So. 2d 1185, 1187 (Fla. 1995).

Similarly, "e-mail headers are not 'prepared' with the intent to 'perpetuate, communicate, or formalize knowledge of some type.'"[51] E-mail headers are different from mail or phone logs in that e-mails headers are recorded as "multiple independent entries" rather than one complete log constituted by a single document; plus, e-mail headers are incidental to the technology rather than deliberately maintained.[52]

Some of the Florida Supreme Court's discussion was devoted to the effect of the City of Clearwater's "Computer Resources Use Policy," which informed employees that the computer resources are property of the City and the users have no expectation of privacy.[53] As Times Publishing argued, the policy may go to establishing no reasonable expectation of privacy.[54] However, the individuals did not assert a privacy right, and Times Publishing based its

---

[51] State v. City of Clearwater, 863 So. 2d 149, 155 (Fla. 2003) (*citing* Shevin v. Byron, Harless, Schaffer, Reid & Associates, Inc., 379 So. 2d 633, 640 (Fla. 1980)).

[52] State v. City of Clearwater, 863 So.2d 149, 155 (Fla. 2003).

[53] *Id.* at 154.

[54] *Id.*

right of access on a public records basis.[55] "Florida courts liberally interpret the [Public Records] Statute, and private citizens are entitled to inspect and copy public records unless the records are specifically exempted. The Second District [and the Florida Supreme Court] did not find that personal e-mail was exempt under the public-records statute; instead [they] determined that personal e-mail did not fall under the definition of public records."[56] Furthermore, the Florida Supreme Court found that the City's policy could not affect whether the e-mail was a public record because it was preempted by the constitutional and statutory definition of public records.[57] The definition of public records cannot be expanded to include "personal" documents by a municipality's policy, in

---

[55] *Id.*

[56] Patricia A. Zagami, J. Scott Slater, & Elizabeth G. Bourlon, *Recent Development: Public Records & Meetings*, 32 Stetson L. Rev. 697, 698 (2003).

[57] State v. City of Clearwater, 863 So. 2d 149, 154-155 (Fla. 2003) (*citing* Times Publishing, 830 So. 2d at 846. *Cf.* Tribune Co. v. Cannella, 458 So. 2d 1075, 1077 (Fla. 1984) (stating that a "fundamental principle that a municipality may not act in an area preempted by the legislature" and holding that the Public Records Act preempted the City of Tampa's regulation that delayed the production of requested personnel records)).

which an employee waives a right of privacy in e-mail on government computer systems.[58]

V. Expectation of Privacy

Views have varied greatly on how to view e-mail in terms of a privacy expectation. Some considered e-mail to be like a personal telephone call, where there is typically a relatively high expectation of privacy.[59] Others believe that, absent additional security measures such as encryption, e-mail is equivalent to the old-fashioned penny-postcard.[60] Under the postcard analogy, there is absolutely no reasonable expectation of privacy because anyone along the route between the sender and intended recipient can clearly read the unconcealed message.[61] The

---

[58] *Id.*

[59] "No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." Katz v. United States, 389 U.S. 347, 352 (1967) (footnotes omitted).

[60] Interview with Ben F. Oveton, Senior Justice, Florida Supreme Court in Gainesville, Fla. (Feb. 12, 2004).

[61] *Id.*

proponents of the postcard analogy argue that clear-text e-mails can be read by anyone along the multiple nodes through which an e-mail passes on the way to its destination.[62] Simply viewing the e-mail headers will supply the address of the intended recipient, the origin, and the history of stops along the way.[63] The e-mail message body is merely one more file to read attached with the header. However, the advocates of the phone call analogy claim that opening the files to read them requires a deliberate act like wiretapping a phone at a telephone company junction box or like opening a sealed envelope. The courts have wavered over defining the expectation of privacy. The Florida Supreme Court seems to analogize e-mail to a letter or memo rather frequently with respect to public records,[64] which implies conversely that there may be

---

[62] *Id.*

[63] The technology needed to do this is widely available for public use at little cost, even though it may not be widely used for various reasons. This is not an instance where the government would require the use of an expensive or advanced technology. *See* Kyllo v. United States, 533 U.S. 27 (2001) (Law enforcement used expensive military-grade thermal imaging device, which not was not in widespread public use, to observe heat escaping from a home where marijuana was being grown.)

[64] "These approaches are no different from the present obligation on judicial officials and employees who receive or send communications in connection with the transaction

at least some degree of privacy for governmental employees in e-mail which is not required to be public accessible. Once again, the privacy here is only a protection from unreasonable governmental intrusion.[65] The government may vitiate an expectation of privacy by a waiver agreement, such as the City of Clearwater's "Computer Resources Use Policy."[66] Public universities also notify computer system users that they can expect their privacy to be limited.[67] Further, whether a public employee or a private citizen,

---

of official business, be it by memo or letter." In re Amendments to Rule of Judicial Admin. 2.051 - Pub. Access to Judicial Records, 651 So. 2d 1185, 1187 (Fla. 1995).

[65] Fla. Const. art. I, § 24.

[66] State v. City of Clearwater, 863 So. 2d 149, 154 (Fla. 2003).

[67] *University of Florida's Acceptable Use Policy* (2003), at http://www.it.ufl.edu/policies/aupolicy.html. ("Users should also be aware that their uses of university computing resources are not completely private. While the university does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the university's computing resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the rendition of service. The university may also specifically monitor the activity and accounts of individual users of university computing resources, including individual login sessions and the content of individual communications, without notice, . . ."). *Policies for Use of Gatorlink* (1999), at http://www.gatorlink.ufl.edu/policy.html ("GatorLink Management has the right to monitor all activity on a computer system including individual sessions.").

governmental intrusion into e-mails is not unreasonable if proper channels and safeguards are in place, such as when law enforcement obtains a search warrant for conducting electronic surveillance.

VI. Private Employers

Private employers are virtually unrestricted in monitoring e-mail on their systems. Since private employers own the equipment and are not restricted like the state by the constitutional right to privacy, they may read e-mails on the computers systems as they please. Employers often have contracts or policies which give employees notice that all information created, sent, or received with their resources is property of the employer. Employers may also feel justified in monitor electronic communications in order to supervise quality of work and to ensure that the employee is rendering services in exchange for compensation paid. Additionally, the employer may wish to avoid liability for abuses of Internet resources, and reasonable supervision of employees may serve as a defense to some tort claims under a vicarious liability theory.

The remedies available to a private employee for an employer reading the employee's personal e-mail lie within

the realm of tort law.[68] These privacy torts include: appropriation;[69] intrusion;[70] public disclosure of private facts;[71] false light in the public eye;[72] and, invasion of privacy.[73] In the 1944 case of *Casin v. Baskin*,[74] the Florida Supreme Court held that an action for invasion of the right to privacy was cognizable in Florida. Unfortunately, despite a buffet of tort law to choose from, it can be difficult to select one that applies to a technological invasion of privacy. Some information may be given voluntarily to one party for a limited purpose but then be used by another party or used for offensive purpose. Other uses may be offensive but not meet other requirements under the tort such as "wide dissemination" or falsity. This shaky ground for stating claims is a

---

[68] The Honorable Ben F. Overton & Katherine E. Giddings, *Article: The Right to 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, 41 (1997).

[69] *Id.*

[70] *Id.* at 42.

[71] *Id.*

[72] *Id.* at 42-43.

[73] *Id.* at 43.

[74] Cason v. Baskin, 155 Fla. 198 (Fla. 1944) (Majorie Kinnan Rawling's book *Cross Creek* used the name and a character portrayal of the author's friend).

problem, especially when the employer may counterclaim with old torts that are being resurrected to apply in new circumstances, like with cybertrespass where claims for trespass to chattels and conversion may arise out of unauthorized use of a computer system so as to interfere with a property right.[75]

While the ability for an employee to prevent an employer from accessing personal e-mail on a work computer may be limited, there are more options available when a stranger snoops into one's e-mail. Federal protection from unauthorized access via criminal law in the Chapter 121 "Stored Wire and Electronic Communications and Transactional Records Access":

> § 2701. Unlawful access to stored communications
>
> (a) Offense. Except as provided in subsection (c) of this section whoever--
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.
>
> [Subsection (b) Punishment has been omitted]

[75] Lecture in Unfair Competition by Thomas Cotter, at Gainesville, Fla. (Apr. 14, 2004).

(c) Exceptions. Subsection (a) of this section does not apply with respect to conduct authorized--

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.[76]

Florida has also provided nearly identical protection in its statute devoted to "Security of Communications":

§ 934.21. **Unlawful access to stored communications**; penalties

(1) Except as provided in subsection (3), whoever:

(a) Intentionally **accesses** without authorization a facility through which an electronic **communication** service is provided, or

(b) Intentionally exceeds an authorization to **access** such facility,

and thereby obtains, alters, or prevents authorized **access** to a wire or electronic **communication** while it is in electronic storage in such system shall be punished as provided in subsection (2).

(2) The punishment for an offense under subsection (1) is as follows:

(a) If the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, the person is:

1. In the case of a first offense under this subsection, guilty of a misdemeanor of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 934.41.

2. In the case of any subsequent offense under this subsection, guilty of a felony of the third degree, punishable as provided in s.

[76] 18 USCS § 2701 (2004).

775.082, s. 775.083, s. 775.084, or s. 934.41.

(b) In any other case, the person is guilty of a misdemeanor of the second degree, punishable as provided in s. 775.082 or s. 775.083.

(3) Subsection (1) does not apply with respect to conduct authorized:
(a) By the person or entity providing a wire or electronic **communications** service;
(b) By a user of a wire or electronic **communications** service with respect to a **communication** of or intended for that user; or
(c) In s. 934.09, s. 934.23, or s. 934.24.[77]

The protection via criminal law serves as a strong deterrent for would-be snoops, thus the individuals expectation of privacy in e-mail might be increased by awareness of legal safeguards. The statutes may help individuals protect their privacy, even thought the primary purposes of these criminal laws it to prevent fraud, theft of confidential government and business information, trade secret misappropriation, and sabotage of computer systems.

VII. Attorney-Client Confidentiality and Discovery

With the current state of the law, it is prudent to take every precaution to protect clients from waiving the privilege of confidentiality between an attorney and client.[78] The first recommendation is to not use e-mail to

[77] Fla. Stat. § 934.21 (2004).

[78] Lecture by Lyrissa Lidsky, *Ethics and Internet*

communicate with clients, and to warn clients not to send confidential information via e-mail on any website or publication in which the attorney's e-mail address is listed.[79] Explain the risks to confidentiality posed by correspondence by e-mail.[80] Second, if e-mail is a preferred medium of communication, then it is essential to set up a secure link or a system of encryption to protect the content.[81] A prudent attorney should password protect computers, particularly laptops which might be more easily lost or stolen.[82] E-mail communications are subject to the highly-valued attorney-client privilege in Florida and most other jurisdictions, but case law is still developing since there are relative few cases.[83] While it used to be debated

---

Defamation, at Gainesville, Fla. (Aug. 25, 2003).

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] A search on the Lexis-Nexis system yielded only one written opinon in Florida and about 170 opinions nationally when using search terms "attorney-client privilege /s e-mail." In Florida: Omega Consulting Group, Inc. v. Templeton, 805 So. 2d 1058, 2002 Fla. App. LEXIS 396, 27 Fla. L. Weekly D 246 (Fla. 4th DCA 2002) (privilege in e-mails waived because, although given to attorney, attorney not the only recipient of communication between insured and insurer).

whether e-mail should be used at all in the practice of law, it has become more common with the increased expectation of privacy from the criminalization of intercepting communications.[84]

E-mail is subject to discovery requests just like any other document produced which is related to a matter in concern. Penalties may be imposed for failure to turn over e-mails, and if e-mails records are kept in the regular course of business then a party may even be required to produce documents from a backup system.[85]

Those records which also happen to be public records are even more susceptible to the discovery process. Income, benefits, and other detailed information is available as a check on government, but that information may also be used for personal gain in private litigation. In *Barron v. Florida Freedom Newspapers*,[86] Supreme Court of Florida held that civil and criminal trials in Florida are public events and adhere to well established common law

---

[84] Lecture by Lyrissa Lidsky, *Ethics and Internet Defamation*, at Gainesville, Fla. (Aug. 25, 2003).

[85] *See* Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99 (2d Cir. 2002).

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

right of access to court proceedings and records.[87] Closure of court proceedings and records should only occur when necessary to comply with established public policy set forth in the constitution, statutes, rules, or case law.[88] So, the spouse in this divorce case was able to gather information about her husband's assets and such from public records and then additional medical information that she obtained during discovery also become public record through the judicial reporting process.

One important role that e-mail brings into the courts is the notion of electronic discovery. Many litigants and criminal attorneys insist on having original documents in electronic form.[89] Requests are made for production of backup records in addition to printed copies.[90] Comparisons may be made for tell-tale signs alterations or deletions.[91] Sometimes electronic documents contain information that is kept as part of the file that is not visible in a printed document – even the time and date stamp of the file or the

---

[87] *Id*. at 116.

[88] *Id*. at 118.

[89] Lecture by Douglas Rehman, *Electronic Discovery*, at Gainesville, Fla. (Mar. 20, 2003).

[90] *Id*.

[91] *Id*.

registered user of the computer that produced the document may be of substantial importance in some matters.[92] Additionally, electronic form can save paper, waste, and expense; plus, documents on a computer are more easily searchable.[93]

VIII. Normative Discussion

Many unresolved issues still exist. Such concerns include practicability of self-policing, lack of uniformity, feasibility of maintaining electronic records, safety and security, and secondary usage of information.

How practical is self-policing in the role of government accountability? The potential exists for corrupt individuals to determine for themselves what is personal, when the governmental entity designates the employee as the person to make such a distinction. Additionally, Times Publishing challenged the City's practice of allowing its employees to filter out their personal e-mail from public e-mail.[94] Under Florida

---

[92] *Id.*

[93] *Id.*

[94] See Times Publ'g Co. v. City of Clearwater, 830 So. 2d 844 (Fla. 2d DCA 2002).

Statutes, either the records custodian or a designee can review e-mail and specify what is nonpublic.[95] The City's procedures designated employees to sort their own e-mail, thereby satisfying the statute's requirements. This is certainly more reasonable than expecting the state government to have one appointee responsible for deciding what records should be public accessible (not person or exempt). Of course, the courts should not be overwhelmed with making such decisions either; and, the courts defer to the legislature. Along the same lines, by letting each agency work with its own policy it creates a lack of uniformity in the law, and yet with the substantial guideline provided by the legislature a needed aspect of flexibility is built into the public records law. The current system has been working fine for a long time.

Flexibility is key when it comes to determining methods of storage for e-mail records. The courts require that agencies do the best they can with what is technologically feasible. Naturally, feasible has a reasonable cost factor built-in. Sorting, storage medium and duration, accessibility and form are all concerns relating to whether servers can handle the storage capacity needed to maintain all e-mails. Therefore, selectivity is

[95] Fla. Stat. $ S 119.021.

important with regular disposal of nonessential records. However, in reality, many entities such as universities do not enforce the public records policy adequately because employees are not informed of their responsibilities.

Security is a big topic after the terrorist attacks of September 11, 2001. Some feel that it is inappropriate to restrict government access to information more than it is for non-governmental/corporate access. The Patriot Act was designed to counteract this problem but has embraced great criticism from both advocates of privacy rights and those seeking to beef-up national and state security. Some laws do protect private information that can be used for commercial advantage in both a local and international environment. Unfair competition and a trade secret laws exist on the state level because of Florida's adoption of the Uniform Trade Secrets Act.

There is a demand for legislative action for protection against private persons wishing to intrude on individual privacy. One push is to control the sale of information by state agencies. Problems exist with secondary usage of information – use of information for something other than the intended purpose for which it was disclosed. Public records can be used for any purpose, not just to supervise government.

IX. Conclusion

In conclusion, e-mail is merely a form of communication which supplies a technologically advanced channel for transport and medium for storage. In essence, the traditional public records laws are adequate without further adaptation; in fact, Florida law has already provided for electronic records in the statute directly. Content is more relevant than the form. Discovery and privilege rules remain consistent with their application to non-electronic information, although electronic discovery may be requested in addition to paper copies.

E-mail does make communication easier for the sender and recipient, but it also makes it more feasible for others to access personal information. Merely accessing the information is enough to outrage some people, but often the harm does not stop there. Once information has been disclosed there is an overwhelming lack of control over with whom the information may be shared and how it may be used. Perhaps this is one aspect of our privacy that the legislature should consider protecting by new statutes. Or, maybe, another constitutional amendment can provide privacy protection against other individuals; unfortunately, the problem is finding a way to do so

without interfering with federally protected First Amendment rights to free speech and without abridging the right of the press and public to access information.