Introduction

As public internet use expanded in the 1990s, governments responded by publishing information online to inform citizens about their rights and responsibilities and to save resources traditionally channeled toward answering questions and printing publications.1 Spurred by legislation, government agencies turned their attention to technological investments that allow online submission and collection of paperwork.

Today, members of the public may use the internet to determine eligibility for benefits under thousands of government programs, file tax returns, comment on proposed regulations, search government job vacancies, or even reserve a camping spot in a national park.2 New technologies help streamline internal processes for sharing information among different agencies and levels of government, simplify and reduce paperwork involved in procurement, and provide payroll and benefit information to employees online.3

State and local governments have followed the paperless trend, balancing issues of privacy, security and efficiency as they digitize public documents and large amounts of governmental data for online availability.4 For example, Boston developed an online portal and call center, called Citizens Connect, to increase public access to city services.5 Its mobile phone application allows smartphone users to report potholes, graffiti, and other problems directly to City Hall, complete with GPS coordinates.6 The 311 system in Miami-Dade County, Florida, handles more than 400 types of service requests and accepts photos of incidents requiring the attention of enforcement officials.7

In addition to improving public access to government activities, changing technology and the paperless trend have caused many local governments to replace courier-delivered agenda binders with laptops and tablet computers, virtually eliminating printing and delivery costs, improving efficiency, and promoting environmental stewardship.8

Paperless Government: A Catalyst for Efficiency

Although paperless government has moved to the forefront in discussions of governmental efficiency and sustainability, it is not a new phenomenon. The federal government solidified its commitment to the ideals of such a system in 1998 with the Government Paperwork Elimination Act.9 Over time, with the evolution of technology and the growth of environmental values, the concept has expanded, with the Office of Budget and Management (OBM) taking a central role in furthering the act’s core principles.10 The federal government’s cost-effective innovations and greener office practices highlight the opportunities for all governments to encourage environmental values and benefit from increased functional efficiency through state and/or local paperless initiatives.

The government of Fairfax County, Virginia, praised nationally for its innovation, has seized these opportunities and implemented an entire system of “e-government.”11 The system boasts 24-hour internet accessibility as well as kiosk accessibility in county buildings.12 Electronic access to the county government allows the public to “pay taxes, search for government facilities, access court information, and register for parks and recreation activities, all without … leaving home.”13 The government itself
constitutes merely one beneficiary of a paperless system; individual citizens receive similar benefits by saving time and personal resources. 14

Even small, localized governmental bodies benefit from transitioning to a paperless system. In 2010, the City Council of Yuba City, California, voted unanimously to cease printing meeting agendas, proposed budgets and adopted budgets. 15 The city saved thousands of dollars and reams of paper by implementing this change. 16 Meeting attendees use electronic tablet devices to access documents.

Even rural towns can take advantage of paperless initiatives, such as intermunicipal (shared services) agreements to capitalize on the long-term cost savings. For example, in Maine, a largely rural state, several libraries facing shrinking budgets and limited space to store all of their print resources have entered into partnerships to store paper documents as well as consolidate their digital collections. This not only saves space and money but also helps libraries spread information to a wider public. 17

Governments at every level have recently begun to heavily utilize social media and social networking. Currently, almost 70 percent of all government workplaces are using some form of social media, with 65 percent using more than one. 18 Social media can be used by governments for a variety of reasons, including providing timely and cost-effective communications, creating a real-time public record of project information, increasing public participation in the democratic process, promoting “sunshine” in government activities, garnering support for upcoming government projects, and even fostering economic development. 19

Legal Considerations and Paperless Government

Despite the temptation to promptly follow the trend of going paperless, governmental entities must examine the legal implications carefully. Of paramount importance is the system’s ability to retain integrity and authenticity so that originality may be easily verifiable. 20 The system must also guarantee retention of complete, unaltered records as required by law. 21 Lastly, the system’s security must safeguard certain information while maintaining accessibility to the public record. 22

Governmental entities manage public records pursuant to statutory requirements. 23 Traditionally, documents were stored as paper records and then as microfiche. The development of new technologies allows for more efficient indexing and information recall through electronic record keeping. This is an attractive option for cities and counties facing strict limits on space and funding, as well as municipalities seeking to promote environmental sustainability.

However, the decision to revamp an existing system requires a careful examination of state and local statutory requirements with regard to what constitutes a “record,” records retention in general, and the “public” or “confidential” nature of certain records.

Records Retention: The What and the How

Transitioning to electronic record keeping may require governments to create electronic copies of all existing paper records, a seemingly daunting task for many. However, some offices have established a policy to effectuate a gradual transition, which requires only new records to be produced in electronic form.

In Massachusetts, a public record includes “books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by any ... [municipal] officer or employee.” 24 Generally, governmental entities should expect to retain such documents (although particular exceptions do exist). Those designing a plan to transition to paperless record keeping must consult applicable local statutes to determine retention requirements in their individual jurisdictions, such as whether the law allows for electronic retention of a certain type of record or whether that record must be retained in some tangible form.

In regard to records that are already in electronic form, going paperless requires determining which emails must be kept as part of the public record. An email, like traditional nonelectronic communications, may offer insight into a governmental action on a matter of public concern. 25 An email becomes a part of the public record as though it were a work-related discourse conducted through traditional paper correspondence. Generally, an email’s content determines when recordation and retention are appropriate. 26 Virginia’s guidelines

Patricia E. Salkin is dean of the Touro College Jacob D. Fuchsberg Law Center. Prior to that, Salkin was the Raymond & Ella Smith Distinguished Professor of Law, as well as associate dean and director of the Government Law Center of Albany Law School. Dean Salkin is a current member of the N.Y. State Bar Association’s Standing Committee on Legal Education and Admission to the Bar and a member of the City Bar’s Task Force on New Lawyers in a Changing Profession. She is a past chair of the American Association of Law Schools State & Local Government Law Section and is the author of hundreds of books, articles and columns. She is an appointed member of the National Environmental Justice Advisory Council, a federal advisory committee to the U.S. Environmental Protection Agency.

Howard F. Gross is the founder and president of E-BizDocs, Inc., a document management company located in Albany, N.Y., that focuses on paperless solutions for governments at all levels. During its 12 years of operation, the company has digitized millions of public records and documents, enhancing government efficiency. Gross is a graduate of Pace University and the Lally School of Management and Technology at Rensselaer Polytechnic Institute in Troy, N.Y.

This article is adapted from Greening Local Government: Legal Strategies for Promoting Sustainability, Efficiency and Fiscal Savings (ABA Publishing, 2012).
diagram an analytical framework for discerning whether a particular email must be retained. The graph provides guidance by mapping out certain determinative factors in classifying an email for retention or deletion that will likely overlap with other state regulations. Although the graph provides general principles relevant to all states, those defining public record in a similar manner as Virginia will necessarily find the framework to be of greater relevance.

New York County does not restrict the way that a clerk retains records, requiring that the clerk “provide … all books, files and other necessary equipment for the filing, recording and depositing of documents, maps, papers in action and special proceedings of both civil and criminal nature, judgment and lien docket and books for the indexing of the same.” This language seemingly allows the county clerk to electronically deposit records. Municipal statutes that fail to explicitly designate the proper form of records retention naturally give rise to the inference that an electronic system is legally permissible.

Similarly, statutory language establishes the level of discretion given to the record keeping officer. In New York, the clerk “coordinate[s] the development … [and] oversee[s]” the system while also “coordinat[ing] legal disposition” of records. This language grants the clerk broad discretion and almost certainly allows for the creation of an electronic system. Some states, however, may not address the clerk’s discretion in designing an electronic system. In such cases, an examination of the state’s technology statutes may provide guidance.

The Evolution of Freedom of Information Laws for Paperless Governments

Since the passage of the Freedom of Information Act (FOIA) in 1966, the definition of record has evolved to accommodate technological advances and presently includes “any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format.”

Each state also has its own freedom of information law (FOIL) or public records law, necessitating a state-specific analysis to ascertain the implications of a particular law’s requirements for public access in an electronic record keeping system. Some states guarantee public access to certain records regardless of form. Obtaining information should be no more difficult under an electronic system than it had been under the traditional system.

Some states directly address the relationship between FOILs and electronic records. For example, in New York, municipal officials are directed to distinguish a record based only on content, i.e., without regard for the record’s form. When the content is covered by the applicable FOIL, the government must produce the record for the request party. The government must additionally consider the other ways in which a FOIL affects electronic records. For example, records produced in electronic form “shall not be encrypted.”

Overbreadth is a potential issue with all FOIL requests but comes to the forefront with an electronic system because indexing may produce thousands of results. The New York FOIL provides that records must be made available following a “request for a record reasonably described[,]” New York’s Committee on Open Government (Committee) issued an advisory opinion clarifying the definition of reasonable for purposes of a FOIL request, stating that a reasonable request “adequate[ly] enable[s] the agency to locate the records” and could not be denied for overbreadth absent an agency showing that the “descriptions were insufficient for purposes of locating and identifying the documents sought.”

A 2008 amendment to New York’s FOIL demanded agency “retriev[al] or extract[ion] of a record or data maintained in a computer storage system” if possible with “reasonable effort.” The Committee subsequently issued a “primer” on the implications of a FOIL with an electronic system, which emphasized the decisive nature of individual circumstances in determining a request’s reasonableness and required that locating the desired records must be possible through “reasonable effort.”

Unfortunately, these definitions do not solve the overbreadth problem with electronic indexing as some searches yield tens of thousands of results. Specifically, agencies may have to read each individual result to verify whether it contains a disclosure prohibition. This could significantly burden a government entity when, for example, a FOIL request for emails involving a specific person generates over 175,000 hits. The Committee implied that the interpretation of reasonable will continue to evolve with changing technology and suggested that denial may be justified if reviewing the documents would be “overly burdensome, time consuming or costly.” Most recently, New York’s Supreme Court Appellate Division,
in an attempt to clarify reasonableness, effectively reiterated the vague definitions of the past, stating that a reasonable request would “enable the agency to identify and produce the record.”

Additionally, local governments need to be aware of their obligations under the rules of discovery for litigation that may arise in the future. Governmental entities are required to produce all required records, including electronic records during litigation discovery periods.50

Paperless governments give rise to two major nontraditional security threats: cyber invasions and improper destruction of electronic information.

The Legal Weight of Electronic Signatures
A record may sometimes require authorization to formalize a party’s assent to its content. Defining the scope of an electronic records retention system requires an evaluation of the legal force carried by an electronic signature.51 Federal and state e-signature laws approach the issue in various ways.52

Florida’s Electronic Signatures Act of 1996 served to enhance the public’s confidence in the legitimacy of electronic signatures.53 The act provides the guidance necessary to implement a trustworthy and legitimate e-signature system. An electronic signature must be “executed … with an intent to authenticate a writing” and be “logically associated with such a writing” to carry legal force equivalent to a written signature.54 To further emphasize the integrity of its e-signature laws, the act borrows from the federal e-signature legislation, the Uniform Electronic Transactions Act, declaring that an electronic record or signature is enforceable, may be used as evidence in a proceeding, and may not be disregarded and cyber theft.55 For example, a governmental entity may face liability exposure when a security breach reveals or publicizes confidential information.56 Destroying electronic records is more challenging than shredding a traditional paper document, and its multistep process will require legal regulation to ensure adequate destruction.

Some states have addressed the issue of cyber invasions by providing guidance on security techniques. For example, Colorado’s records retention schedule requires a municipality to keep certain computer system records for security purposes, including “access requests, authorizations, encryption keys, journals, password documentation, reports, system access logs and other access control records.”57 It also provides instruction on how long to retain each type of record.60 The North Dakota Office of Management and Budget requires system administrators to “set access privileges to protect records from unauthorized users.”61 The New York State Office of Cyber Security (NYSOCS) is responsible for “identify[ing] and mitiga[ng] … vulnerabilit[ies]” in order to “protect[] the State’s cyber security infrastructure.”62 The NYSOCS guide for governments in transition is relevant for all jurisdictions as it addresses general concerns common to all paperless systems and represents the product of a collaborative effort with the Multi-State Information Sharing and Analysis Center (MS-ISAC), a national organization “focused on enhancing our cyber posture.”63 The guide emphasizes a municipality’s duty to protect stored information and the costs associated with that responsibility.64 Different security techniques are more or less costly depending on a variety of factors, but using the methods in conjunction with one another based on the importance or confidentiality of the recorded information will minimize costs.65 An electronic system raises several general security concerns for all jurisdictions, including physical protection of equipment, law enforcement, protection against cyber-invasions, restriction and control of accessibility, and education for system users on detecting and avoiding security breaches. The MS-ISAC has online training sessions available for local governments.66

The destruction of public records presents another legal challenge for governmental entities seeking to become paperless because clicking “delete” does not destroy a document.67 Unfortunately, it is “virtually impossible to completely destroy an electronic document.”68 Until a file is written over, all of its information is still available and recoverable; the Department of Defense recommends that data be written over seven times to ensure successful destruction.69 There are various techniques for destroying files, ranging in cost and effectiveness.70

Some states outline minimum procedural standards for destroying electronic records. Texas law does not require a certain type of data removal, granting discretion to municipalities as long as the records are “disposed of in a manner that ensures protection of any confidential information[.]”71 This
statutory framework allows more autonomy at the local level but still ensures proper destruction. Appropriate destruction techniques for confidential records in Florida “include physical destruction of storage media such as by shredding, crushing, or incineration; high-level overwriting that renders the data unrecoverable; or degaussing/demagnetizing.”72 However, Florida’s pro-recycling policy would likely favor “scrubbing.”73 An MS-ISAC supplement on destruction of electronic media provides general guidance for paperless governments. It recommends scrubbing or wiping of all electronic devices such as hard drives or cellphones but advises physical destruction of CDs, DVDs and faulty hard drives under warranty.74 It also suggests that governments keep a destruction log to audit destruction.75

Related to the destruction of electronic records is the problem that some governments may encounter with document retrieval. Converting traditional files into electronic copies is a fairly easy and straightforward process; but just as it is important to name or index paper files, it is equally important to do the same with digitized records. Governments need to establish strict file-naming policies for all converted files. Governments that use a document management program aren’t likely to have this problem as a majority of these programs use a “lock-down system” that automatically institutes a uniform naming procedure for files and prevents users from placing their own, possibly nonuniform (and therefore difficult to retrieve) names on files.76

Conclusion
The shift to paperless governments represents a new era, marked by efficiency and cost-cutting but also motivated by sustainability concerns. As more and more governments move in this direction, government attorneys must be mindful of records retention, accessibility and privacy issues so that proper safeguards are put into place to ensure compliance with applicable state and federal laws.

Endnotes
6 Id.
12. Id.
13. Id.
14. Id.
15. Id.
16. Id.
19. Governments need to temper their reliance on the information they provide through social media because such media can be unrepresentative and skewed in the direction of a vocal minority. Similarly, governments need to be wary of the variety of legal and ethical issues that surround the use of social media, such as First Amendment concerns, open meeting laws and Freedom of Information Act requests, discriminatory usage, and possible conflicts of interest. See Lyrissa B. Lid- sky, Government Sponsored Social Media and the Public Forum Doctrine Under the First Amendment: Perils and Pitfalls, 2 Pub. Law. 19:22 (Summer 2011).
21. Id.
22. Id.
functions and responsibilities of public employees, e-mail should be treated in most respects just like paper in terms of public rights of access, retention and disposal.

26. See also COLO. DEP’T OF PERSONNEL & ADMIN., COLORADO MUNICIPAL RECORDS RETENTION SCHEDULE § 9.5-40(B) (2010) available at www.colorado.gov/dpa/doit/archives/rmm/MuniRMM/ (expressly designating a time period for retention based on the type of record).


28. Id. at 2.

29. N.Y. COUNTY LAW § 525 (McKinney 2004).

30. However, the municipality, when designing a plan, should consider historic documents because statutory guidelines may prohibit or create additional limitations on their destruction altogether. See id. § 57.25.

31. Id. § 57.19.


36. See 13 TEX. ADMIN. CODE § 7.79 (“An electronic recordkeeping system must not provide an impediment to access to public records.”).

37. Id.

38. See, e.g., N.Y. STATE TECH. LAW § 308(1) (“Electronic records shall be considered and treated as any other records for the purpose of the freedom of information law.”).

39. N.Y. PUB. OFF. LAW § 86(4) (McKinney 2010).

40. Id.

41. Id. § 89(3)(a).


43. N.Y. PUB. OFF. LAW § 89(3)(a); see also N.Y. DEP’T OF STATE, COMM. ON OPEN GOV’T, PRIMER ON E-FOIL ISSUES (Dec. 2009) (“If the Town maintains all such records in a file or group of files that are retrievable on the basis of the terms of your request, I believe that you would have met the requirements that the records be reasonably described.”).


45. Id. at 3.

46. Id.

47. Id.

48. Id. at 5.


51. The scope of records allowed in a paperless system would be limited if electronic signatures held no legal force. For example, residents would not be allowed to submit tax or registration forms online because they require signatures.


53. FLA. STAT. ANN. § 668.002(2) (West 2010).

54. Id. §§ 668.003(4), 668.004.

55. Id. §§ 668.50(7), 668.50(13).

56. See, e.g., Electronic Signatures and Records Act, N.Y. STATE TECH. LAW §§ 301–09 (McKinney 2010).


59. COLO. DEP’T OF PERSONNEL & ADMIN., supra note 26, § 9-5.20.

60. Id. § 9-5.20(A)–(C).


62. N.Y. OFFICE OF CYBER SEC., ABOUT OCS, www.cscic.state.ny.us/about.


64. Id. at 3.

65. Id. The guide discusses the “Top Ten Cyber Security Action Items,” a list that includes regular reviews of applicable laws and problem-avoidance techniques, among others. Id. at 3–6.

66. Id. at 6.


68. Leavitt, supra note 67.

69. Id.

70. Id. Leavitt goes on to discuss destruction methods, the most costly involving physical destruction of a storage device (i.e., shredding a hard drive). “‘Scrubbers’ present a more affordable option because they delete the file and rewrite over the deleted file multiple times.

71. 13 TEX. ADMIN. CODE § 7.78(b) (2010). Destruction of records from a particular system may implicate additional requirements, such as a record contained within an optical Write-Once-Read-Many system, where “the information may be overwritten to obliterate the original image, leaving no evidence of the original information, or... all of the indices, pages, or documents on a disk, other than the expunged document(s), must be rewritten to a new disk and the old disk must be physically destroyed.” Id. § 7.78(c)(1).


73. Id. r. 1-24.003(10).

74. See MULTI-STATE INFO. SHARING & ANALYSIS CTR., supra note 67.

75. Id. at 6.