A Report by the Attorney General Following an Investigation into Allegations of Criminal Destruction of Email.

I. Introduction

In October 2009, the Secretary of the Commonwealth referred to the Office of the Attorney General ("AGO") a matter involving the email practices of a senior Boston city official. Specifically, the Secretary asked the AGO to investigate whether Michael J. Kineavy, Chief of Policy and Planning for the City of Boston, had committed a crime by deleting emails from his City Hall computer.

The AGO investigation was extensive. The AGO requested and reviewed thousands of pages of documents. It conducted a forensics analysis of Kineavy's computer systems. It also interviewed numerous witnesses, with the last interview taking place in late June 2010.[1]

The investigation focused on a specific task: determining whether Kineavy's deletion of email was a crime. Given all the facts revealed in the investigation, we did not find that the facts supported a criminal case against Kineavy. More specifically, we did not find that his actions warranted a charge of unlawfully destroying public records in violation of G.L. c. 66 § 15.

II. The Statute, Its Purpose and Scope

Since 1851, it has been a crime in Massachusetts to remove or destroy a public record.[2] As part of the broader public records law, the statute's primary purpose is to ensure wide public access to governmental records. See Worcester Telegram & Gazette

[1] The scope of the investigation is set out more fully in the attached addendum.

[2] See St. 1851, § 4 ("Whoever shall be guilty of taking and carrying away any book of record, paper or written document, or of defacing, altering or mutilating same . . . shall forfeit and pay a sum not exceeding fifty dollars").

Corp. v. Chief of Police of Worcester, 436 Mass. 378, 382-383 (2002). The public records law, as a whole, expresses the Legislature's "considered judgment that the public has an interest in knowing whether public servants are carrying out their duties in an efficient and law-abiding manner," and that "greater access to information about the actions of public officers and institutions is increasingly . . . an essential ingredient of public confidence in government." Suffolk Construction Co., Inc. v. Division of Capital Asset Management, 449 Mass. 444, 453 (2007), quoting Attorney General v. Collector of Lynn, 377 Mass. 151, 158 (1979) and New Bedford Standard-Times Publ. Co. v. Clerk of the Third Dist. Ct. of Bristol, 377 Mass. 404, 417 (1979) (Abrams, J., concurring).

The current version of the statute imposes a fine or term of imprisonment on whoever "unlawfully . . . alters, mutilates or destroys any public record." G.L. c. 66, § 15. Although section 15 is broad, three things limit its reach. First, it applies only to "public records." Generally, public records are "documentary material or data, regardless of physical form or characteristics" that are "made or received" by a public official, G.L. c. 4, § 7(26), and the term has been interpreted to include email.[3] There are, however, exemptions to this definition. See G.L. c. 4, § 7, cl. 26 (listing exemptions, such as personnel and medical files and information). Thus, not all materials "made or received" by public officials, whether paper or electronic, are "public records."

Second, section 15 applies only to the "unlawful" destruction of public records. The government is not required to keep all its records forever. Rather, public records are preserved in accordance with maintenance schedules promulgated by the Supervisor of

[3] See SPR Bulletin No. 1-99, February 16, 1999, revised and reissued May 21, 2003, http://www.sec.state.ma.us/arc/arcrmu/rmubul/bul199.htm.

Public Records and the state Records Conservation Board. G.L. c. 66, § 8. Thus, public records may be "lawfully" destroyed.

Third, and most importantly for purposes of this report, section 15, is a criminal statute. To sustain a conviction under it, the prosecution must prove that the person charged had a certain state of mind; that is, it must be proven that the person knew that he or she was "destroying" public records.

III. The Referral

On April 1, 2009, the *Boston Globe* ("the *Globe*") made a public records request to the City of Boston ("City") under G.L. c. 66, § 10, which establishes the public's right of access to public records. The *Globe* requested, among other things, certain defined categories of emails to or from Kineavy between January 1, 2008 and April 1, 2009. A second public records request from the *Globe* on June 26, 2009 sought *all* emails to or from Kineavy between September 1, 2008 and April 1, 2009. In response to these requests, the City's Management and Information Systems ("MIS") Department conducted a search for all of Kineavy's emails retained by the City. The MIS Department located a small number of responsive emails, which were provided to the *Globe.* The small number of produced emails raised concerns that Kineavy may have inappropriately destroyed his emails.

The matter came to the attention of the Secretary of the Commonwealth and the Supervisor of Public Records within his office. The Supervisor, by law, has the authority to "take necessary measures to put the records of the commonwealth, counties, cities or towns in the custody and condition required by law to secure their preservation." G.L. c. 66, § 1. On September 14, 2009, the Secretary ordered the City to seize all of Kineavy's

hardware and software to preserve existing data. The Secretary also ordered the City to hire an independent computer forensics firm to recover all emails from Kineavy's hard drives. After reviewing the matter, the Secretary determined that Kineavy had inappropriately deleted emails from his City Hall computer. On October 21, 2009, the Secretary referred the matter to the AGO to determine whether Kineavy's inappropriate deletion of emails was a crime under G.L. c. 66, § 15; that is, did Kineavy unlawfully destroy emails that were public records?

IV. Facts: City Hall's Email Culture

The investigation revealed a misunderstanding among City Hall employees – both in the Mayor's Office and elsewhere – about how the City's email system worked and how emails were maintained on that system. The prevailing view, supported by language in the City's various email policies, was that the MIS Department "backed-up" emails and that deleted emails were never truly lost. This was simply not true. The MIS Department had backup systems in place, but they were not created to meet the City's record retention obligations. Rather, the systems were designed to provide disaster recovery and to protect against data loss. In fact, if an employee deleted an email and then removed that email from his or her Microsoft Outlook "deleted items" folder – or "double deleted" the email – then the email would be overwritten on the City's servers.

A. Kineavy's Email Practices

Kineavy told investigators that, in his current position, he receives approximately 100 emails each work day. For years, Kineavy stated, he has maintained a daily practice of deleting his emails on his desktop computer and then emptying his deleted items folder in his email program, Microsoft Outlook. He said that he routinely deleted email after he

was finished dealing with it because he wanted to start fresh every day and he believed deleting email on his desktop computer did not result in the actual destruction of the email. Rather, he believed that the emails were saved by the City's MIS Department.

Kinveavy's statements concerning his email practices were consistent with those of his administrative assistant, Cathy Downey. Downey has worked as Kineavy's administrative assistant for the past fifteen years. When interviewed, she confirmed that Kineavy had a long-standing practice of deleting his emails at the end of the work day. Her statement was, in turn, consistent with the results of the AGO forensic analysis of Kineavy's computer hard drives.[4] Additionally, that practice was consistent with Kineavy's generally meticulous work habits, as described by several witnesses.

While Kineavy was meticulous, he was not technologically sophisticated. For example, he did not know how to attach a document to the emails he sent. He also rarely drafted documents on his computer. And he preferred a paper calendar to an electronic one.

In short, the investigation indicated that Kineavy's stated practice of cleaning out email in both his inbox and his "deleted items" folders at the end of every business day was both long-standing and consistent with his work habits. There was no evidence in either the witness statements, or on Kineavy's hard drives, that he "double-deleted" emails with an awareness that he was actually destroying them.[5]

[4] That analysis is more fully described in the addendum to this report.

[5] One witness, identified late in the investigation, had allegedly heard City employees occasionally refer to embarrassing or inappropriate emails as "double delete" emails. From that, he inferred that certain emails had been purposely double deleted, or destroyed. This witness had no specific information about Kineavy's email retention practices, and did not report to or even work in the same department as Kineavy. The witness did, however, identify other current or former City employees who could corroborate his statement. Based on this information, investigators conducted six additional interviews. None of the individuals interviewed corroborated the witness's statement. Instead, they all believed that email could

B. Email Practices of Other City Hall Employees

Kineavy's belief that his emails were saved by the City's MIS Department was echoed during interviews of other City Hall employees. Those employees shared a common belief that "emails are forever" and could not be deleted.

Indeed, complainant and former Boston City Council President, Michael Flaherty, shared many of these same beliefs with respect to the hundreds of emails per day that he received at his City Hall email account.[6] Flaherty's email was routinely reviewed and handled by his staff. Flaherty told investigators that he was not sure what happened to the email after his staffers handled it. He also did not know whether they were deleted or "double deleted," which he thought meant deleting emails from a computer and then deleting them from a server. But he believed, like other City employees, that City Council computers were backed-up and that the MIS Department was responsible for backing them up. Again, like others, he did not know precisely how the system worked and did not have any specific knowledge that the computers were backed up. Flaherty also did not remember receiving formal records retention training or any manuals on the subject.

C. The City's Email Policies and Training

The common belief that emails were forever and could not be destroyed was supported by imprecise language in the City's email policies, and by a lack of appropriate training about the City's record retention obligations.

---

not be permanently deleted from City servers. And none of them had any reason to believe that Kineavy had intentionally destroyed email.

[6] Flaherty stated that he had no personal knowledge of how Kineavy managed his email or if Kineavy had special access to back up systems. Rather, all the information he had was from newspaper accounts.

Since 1999, the City has adopted various email policies, published in various contexts. And they all provide at least some support for the mistaken belief among City Hall employees that email was automatically retained by the City's computer systems. For example, the *City of Boston Employee Handbook* (1999) states that "[e]mployees should be aware that all e-mail messages are automatically stored on the City's computer back-up system." Similarly, the City of Boston Management & Information Services *E-Mail and Internet Use Policy*, effective April 2, 1999, provides:

> All e-mail messages and Internet sites visited by City employees are automatically stored on the City's computer back-up systems. Further, employees should be aware that even when a message is deleted, it may exist on a backup tape.

The City's revised *E-Mail Policy*, effective February 2008, provides:

> All e-mail messages received and sent by City employees and affiliates are automatically stored on the City's backup systems. Further, employees and affiliates should be aware that even when a message is deleted, it may exist on a backup tape.

Even after questions were raised about Kineavy's email practices, the City issued a revised email policy containing the following language:

> All e-mail messages received and sent by City employees and affiliates are automatically stored on the City's backup systems for three years on an interim basis. Further, employees and affiliates should be aware that even when a message is deleted, it may exist on a backup tape.

City of Boston Management Information Services E-Mail Policy, effective September 18, 2009.

Finally, and perhaps most importantly, there was only one City policy in place at the time Kineavy was regularly deleting his email that mentioned the City's records retention obligations. It was issued by the City of Boston Archives and Records Management Division – the division with responsibility for

developing and implementing the City's record retention policies and procedures – and it actually *encouraged* employees, in concrete, easy to understand language, to routinely delete emails. The *E-mail Management & Retention Policies*, effective May 21, 2009, states:

> Except as provided below, the maximum retention period for e-mail shall be 90 days after the message is opened/read by its recipient, *but employees are encouraged to delete the messages DAILY, immediately after reading, replying or taking other action concerning them.* Such actions are required of all employees during Records Purge Days. This policy applies to documents attached to e-mail messages as well as to the messages themselves. All opened e-mail older that [sic] 90 days remaining in employees' mailboxes will be automatically purged upon the expiration of this retention period. The retention of e-mail data on back up media will not exceed 90 days.

The policy does reference the City's record retention obligations, but only in an oblique and technical way. It states:

> If the content of an e-mail message or attachments possess business value for longer that [sic] 90 days, and relates to an established records series appearing in the City's General Records Retention and Disposition Schedule (the "Retention Schedule"), it should be made a part of that established file and retained appropriately as per the retention period in the schedules.

The AGO's witness interviews confirmed that this aspect of the policy was not well-understood. Based on the language of the policy itself, it is understandable that City employees could be confused about what they were supposed to be doing with their emails.

This confusion was likely exacerbated by the City's lack of formal training about its record retention policies and obligations. According to witnesses, the only training they received about handling email advised discretion because emails were saved and could be made public if requested. In fact, this encouraged the belief that emails were –

in technical ways that employees did not understand – backed up and saved by the MIS Department.

V. Legal Analysis and Conclusion

The AGO investigation's purpose was to determine whether Kineavy's deletion of email from his City Hall computer was a crime under G.L. c. 66, § 15. Given all the circumstances, particularly the lack of evidence that Kineavy was aware that he was actually "destroying" email by deleting it, and that the City's email policies actually encouraged him to delete daily, we conclude that criminal charges are not warranted.

The relevant language of G.L. c. 66, § 15, states that "[w]hoever unlawfully . . . alters, defaces, mutilates or destroys any public record or violates any provision of this chapter shall be punished by a fine of not less than ten nor more than five hundred dollars, or by imprisonment for not more than one year, or both."[7] So, Kineavy would have committed a crime if he "unlawfully" destroyed emails that were public records.

Criminal statutes generally include an element of intent. For example, the federal equivalent of § 15 makes it a crime to "willfully and unlawfully" destroy a public record. See 18 U.S.C. § 2071. The term "willfully," in the criminal context, means that defendants must not only know that they destroyed a public record, but they must also know that destroying a public record is illegal. See, e.g., Ratzlaf v. U.S., 510 U.S. 135, 141 (1994) ("willfully" means having a "purpose to disobey the law").

[7] The full text of the statute reads: "Whoever unlawfully keeps in his possession any public record or removes it from the room where it is usually kept, or alters, defaces, mutilates or destroys any public record or violates any provision of this chapter shall be punished by a fine of not less than ten nor more than five hundred dollars, or by imprisonment for not more than one year, or both. Any public officer who refuses or neglects to perform any duty required of him by this chapter shall for each month of such neglect or refusal be punished by a fine of not more than twenty dollars." G.L. c. 66, § 15.

In G.L. c. 66, § 15, the Legislature used only the word "unlawfully."[8] See St. 1897, c. 439, § 12 (adding the word "unlawfully" to the statute). Used on its own, "unlawfully" usually means that the crime is a "strict liability" offense. That is, defendants can be convicted simply for doing the prohibited act, even if they are unaware or mistaken about some essential element of the act. See, e.g., G.L. c. 265, § 23 (rape of a child under the age of 16); Commonwealth v. Miller, 385 Mass. 521, 522 (1982) (offense of statutory rape may be committed with or without any knowledge on the defendant's part of the age of the victim). However, even where strict liability is imposed with respect to some essential element of the offense, there is generally a requirement that defendants know they are engaging in an underlying prohibited act. See Lambert v. California, 355 U.S. 225 (1957) (due process may limit strict criminal liability in certain circumstances); Commonwealth v. Buckley, 354 Mass. 508 (1968) (criminal statutes should be construed to avoid due process violations). For example, while a defendant does not have to know he is not licensed to carry a firearm, he does have to know that he is actually carrying a firearm. Commonwealth v. Jackson, 369 Mass. 904, 916 (1976); Commonwealth v. Hampton, 26 Mass. App. Ct. 938, 940 (1988).

Here, the facts are consistent with Kineavy's statement that he did not know that he was "destroying" his emails when he deleted them. Thus, it appears that his practice of deleting his emails at the end of the business day was a business practice, one that the City actively encouraged. Cf. Commonwealth v. Twitchell, 416 Mass. 114, 128 (1993)

[8] When the statute was first enacted in 1851, it did not use the word "unlawfully." Instead, it used the word "guilty." St. 1851, c. 439. The term "guilty" – particularly at the time, when strict liability statutes were uncommon – implies a criminal intent, what is known as *mens rea* or a "guilty mind." See generally Morrisette v. U.S., 342 U.S. 246 (1952) (discussing evolution of strict liability offenses). Therefore, it is unlikely that the Legislature in 1851 meant to impose criminal liability for negligent or accidental "defacing, altering or mutilating" of public records.

(defendants could present affirmative defense that they relied on an arguably misleading Attorney General opinion). Thus, under these circumstances, no criminal charges against Kineavy are warranted because the evidence suggests that he did not know he was "destroying" anything.

VI. Changes at City Hall

Since this investigation began, the City has taken a number of steps both to mitigate the consequences of Kineavy's deletion of his emails and to guard against similar incidents in the future. In response to the Secretary's order, the City hired an independent computer forensics firm, which was able to recover thousands of Kineavy's emails, and the City made the recovered emails available to the public online.[9]

In addition, the City has purchased and installed journaling technology to permanently capture and store all email sent or received by City Hall employees, regardless of whether the email has been deleted by individual employees on their individual work computers. It has also updated its email policies and begun implementing a more comprehensive public records training program for all City employees. For example, on September 17, 2009 – shortly after concerns about Kineavy's email practices were raised – the City issued an *Interim Email Retention Policy*, making it clear that "the sender/recipient may not rely on MIS to fulfill their individual obligations; the sender/recipient must retain emails the content of which is subject to retention requirements."[10]

[9] See http://www.cityofboston.gov/news/kineavy_messages.asp. There is no evidence among the published emails of a lack of transparency or an intent to evade the spirit or letter of the public record laws.

[10] Also helping to clarify matters, the Supervisor of Public Records, on May 12, 2009, approved a general record retention and disposal schedule specific to the City.

VII. Addressing the Gap Between the Law and Evolving Technology

This incident and the subsequent investigation have demonstrated a need to recognize and address the public's demand for government transparency in a world of evolving communication technology.

A. The Evolution of Communication Technology

Massachusetts has had a public records law since 1851. At that time, it was easier to identify and keep public records. Information was written or printed on paper that could be kept in a file or on a shelf, ready for public inspection. Conversations between public employees, or between employees and the public, could not be "records" because there was no way of capturing them, even decades later, when such conversations took place over the telephone. At one time, it was certainly easier to know if a public record had been destroyed: it was a physical act. Paper was ripped out, torn or burned. Words were crossed–out or obliterated.

That has all changed. Instead of talking in person, or picking up a telephone, people now write an email. They often do it casually, just as they would talk on the phone. There is often little sense that they are creating "records" – which implies a certain formality – when using email. And while email is universally used, email technology is not universally understood. As the witness interviews indicated, employees have a sense that email is always saved somewhere, somehow, either on their own hard drives or on a distant server. They do not fully understand where an email goes when they press either the "save" or the "delete" button. And there is a huge amount of email, which has to be managed by both individual users and those maintaining computer networks. For the government, there is a tension between managing its computer systems

efficiently and preserving its records for public inspection. See, e.g., Municipal Records Management Manual, updated June 11, 2010 (issued by the Secretary and recognizing that "[a]s government expands and becomes more complex, so does the creation, maintenance, and preservation of records").

B. The Evolution of the Public's Demand for Transparency

While technology has created efficiencies in conducting government business, its use has also created a heightened concern that business is being conducted out of the public's sight. In the Open Meeting Law context,[11] for example, questions arise about officials allegedly deliberating by email or text before, during or after meetings that are ostensibly open to the public. The answer is not only transparency, but recognition that modern technology and the 160 year-old public records law are not a perfect fit. As technology evolves, the statutory and regulatory framework – as well as the training that implements that framework – must constantly be updated to ensure that government continues to fulfill its obligations of transparency and public responsiveness.

[11] The Open Meeting Law requires, with some exceptions, that meetings of public bodies be open to the public. See G.L. c. 30A, §§ 18-25.

ADDENDUM

The AGO's months-long investigation was extensive and involved at least the following three elements:

I. Document requests: The AGO made six separate document requests to two separate entities. As a result of these requests, the AGO received and reviewed thousands of pages of documents.

II. Witness interviews: The AGO conducted a total of 15 interviews as part of its investigation. The AGO initially interviewed seven City employees, including Kineavy. As the AGO was finalizing its conclusions, another witness with relevant information was identified in March 2010. The interview of that witness led to six additional interviews. The last interview of the investigation was conducted in late June 2010.

III. AGO forensic analysis: The AGO's Computer Crimes Lab conducted a forensic analysis of Kineavy's computer systems to determine whether the forensic evidence was consistent with other information obtained in the investigation. Among other things, the Lab removed and made a digital copy of the two hard drives used by Kineavy during the relevant period. The Lab then analyzed the digital copies. For example, the Lab ran a computer script to recover any folders that may have been deleted from Kineavy's "C drive," and also performed a "signature analysis" to confirm that no file extensions had been changed in an effort to hide the files. An email script was run to recover all email that may have been residing in allocated or unallocated spaces on the hard drives, and email recovery software was used to recover email and email fragments. And "key word" searches were performed to determine if there was evidence on the hard drives of intentional email destruction.