THE SECRETARY'S EMAILS: THE INTERSECTION OF TRANSPARENCY, SECURITY, AND TECHNOLOGY

Joshua Jacobson[*]

Abstract

Transparency laws are designed to inform the public of government workings and to hold government officials accountable to the people. The emergence of email has amplified the government's communicative abilities and simultaneously created major challenges for records management. These challenges were put on full display when it was revealed that Hillary Clinton exclusively used a private email address and server for government business while serving as Secretary of State. The email arrangement Clinton used was permissible under the law at that time, and despite recent changes, government employees may still use private email for non-classified correspondence so long as the messages are copied or forwarded to an official government account.

This Note argues that the present system fails to retain a significant number of government records and puts government email records at risk. Requiring government employees to oversee their own emails results in a conflict of interest. Additionally, records housed on private servers may have inadequate security protections and thus be at risk to hackers. A paradigm shift is needed to ensure that the ever-expanding number of digital communications are preserved and protected.

* J.D. Candidate 2017, University of Florida Levin College of Law; B.S.B.A. 2013, University of Florida. I would like to thank the student and staff editors of the *Florida Law Review* for their diligence and thoughtful edits. Many thanks also to Professor Sharon Elizabeth Rush and Professor Mark Fenster for their support and counsel.

INTRODUCTION

On March 2, 2015, the *New York Times* reported that Hillary Clinton had exclusively used a private email address and server during her time as Secretary of State.[1] The ensuing controversy dominated newspaper headlines for months and led some to call for criminal prosecution.[2] While Clinton responded by turning over thousands of emails, her staff deleted 31,000 emails that it deemed personal.[3]

1. Michael S. Schmidt, *Hillary Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules*, N.Y. TIMES (Mar. 2, 2015), http://www.nytimes.com/2015/03/03/us/politics/hillary-clintons-use-of-private-email-at-state-department-raises-flags.html.

2. *See, e.g.*, *Sen. Chuck Grassley: Hillary Could Be Charged in Email Case*, NEWSMAX (Mar. 31, 2015, 6:47 PM), http://www.newsmax.com/Newsfront/charles-grassley-hillary-clinton-private-email/2015/03/31/id/635635/.

3. Michael S. Schmidt, *Justice Dept. Says Hillary Clinton Had Authority to Delete Certain Emails*, N.Y. TIMES (Sept. 11, 2015), http://www.nytimes.com/2015/09/12/us/justice-dept-says-hillary-clinton-had-authority-to-delete-certain-emails.html.

Strictly speaking, it appears that Clinton's email setup complied with the letter of the law[4]—albeit probably not the spirit.[5] While Clinton was Secretary of State, the law permitted private email use for communications involving government business and did not require that government employees transfer official emails on private accounts to government servers.[6]

This Note does not suggest that Clinton's private email practices were better or worse than those of other government officials. To be sure, Clinton was not the first Secretary of State to use a private email address for government business. Colin Powell relied on a personal email account for communications with "American officials and ambassadors and foreign leaders" during his term as Secretary of State.[7] A recent investigation discovered classified information in some of those emails.[8] Furthermore, a recent survey suggests that many government employees use private email accounts for business.[9]

---

4. *Id.* This is not to say that Clinton complied with the law *if* she knowingly, or with gross negligence, sent emails containing *classified information* on a private server. *See* 18 U.S.C. § 793(f) (2012); Laurie L. Levenson, *Clinton's Email: Unwise, But Likely Not Criminal*, NAT'L L.J., Sept. 21, 2015, LEXIS. Another potentially applicable statute is 18 U.S.C. § 1924, which prohibits removing classified documents "with the intent to retain such documents or materials at an unauthorized location." After an investigation, FBI Director James Comey recommended not prosecuting Clinton, concluding that "no reasonable prosecutor" would bring charges. Press Release, Fed. Bureau of Investigation, Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System (July 5, 2016), https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system. Notwithstanding the FBI's recommendation, Comey admonished Clinton's "extremely reckless" email practices. *Id.*

5. *See* Transparency and Open Government, Memorandum for the Heads of Executive Departments and Agencies (Jan. 21, 2009), *in* 74 Fed. Reg. 4685 (Jan. 26, 2009) ("Transparency promotes accountability and provides information for citizens about what their Government is doing."). Preserving official emails on a private server also deviated from guidelines set forth in the National Archives and Records Administration Bulletin suggesting that emails be preserved in a manner that would "[p]ermit easy and timely retrieval." NAT'L ARCHIVES & RECORDS ADMIN., NARA BULL. NO. 2008-05, GUIDANCE CONCERNING THE USE OF E-MAIL ARCHIVING APPLICATIONS TO STORE E-MAIL (2008), https://www.archives.gov/records-mgmt/bulletins/2008/2008-05.html, *superseded by* NARA BULL. NO. 2011-03 (2010), https://www.archives.gov/records-mgmt/bulletins/2011/2011-03.html.

6. *See infra* notes 66–68 and accompanying text.

7. Josh Gerstein & Tarini Parti, *Colin Powell Relied on Personal Emails While Secretary of State*, POLITICO (Mar. 3, 2015, 2:59 PM), http://www.politico.com/story/2015/03/colin-powell-personal-email-secretary-of-state-115707.

8. Ken Dilanian, *Rice Aides, Powell Also Got Classified Info on Personal Emails*, MSNBC (Feb. 4, 2016, 2:01 PM), http://www.msnbc.com/msnbc/rice-aides-powell-also-got-classified-info-personal-emails.

9. Sharyl Attkisson, *High-Ranking Federal Officials' History of Using Personal Email for Government Business*, DAILY SIGNAL (Mar. 8, 2015), http://dailysignal.com/2015/03/08/high-

Regardless, Clinton's practices exposed a gaping hole in transparency laws in the United States: government officials could conduct their official duties from a private email account and personally retain their email records until someone made a formal request. This gap allowed Clinton's staff—instead of independent State Department employees—to decide for itself what should be disclosed when a formal records request was made.[10]

Government employees using their private email accounts for business is inherently troubling. By communicating outside proper channels, government employees undermine public and institutional oversight and create an incomplete historical record.[11] Furthermore, the practice leaves potentially sensitive information vulnerable to hackers.[12]

Recent amendments to transparency laws sought to bring more records under direct government control,[13] but the fox is still guarding the hen house. Public officials are charged with preserving their own emails for later public inspection. Allowing officials to monitor themselves creates the obvious problem that they will selectively choose which records to preserve, neglecting to preserve records that might hurt their interests if made public.[14]

Moreover, the media's intense scrutiny of Clinton's email revealed the significant shortcomings of the State Department's information technology (IT) systems, as well as other governmental IT systems.[15] Today, many government employees use private email because using their official government email is inconvenient and inefficient.[16] Further, numerous hacks against government agencies have also undermined public confidence in government IT.

---

ranking-federal-officials-history-using-personal-email-government-business/ (noting that thirty-three percent of the survey respondents said they "use personal email for government business at least sometimes"); Brody Mullins, *Survey: Many Government Employees Use Personal Email for Work*, WALL ST. J.: WASH. WIRE (Sept. 1, 2015, 4:19 PM), http://blogs.wsj.com/washwire/2015/09/01/survey-many-government-employees-use-personal-email-for-work/ (discussing a similar survey in which "about 33% of [respondents] said they used their personal accounts for work email at least occasionally").

10. *See* Schmidt, *supra* note 3.

11. *See infra* Section III.A.

12. *See, e.g.*, Byron Tau, *Hillary Clinton's Private Email Server Was Subject to Attempted Attacks*, WALL ST. J., http://www.wsj.com/articles/hillary-clintons-private-email-server-was-subject-to-attempted-attacks-1444323907 (last updated Oct. 9, 2015, 10:36 AM).

13. *See* Presidential and Federal Records Act Amendments of 2014, Pub. L. No. 113-187, 128 Stat. 2003 (codified as amended in scattered sections of 44 U.S.C.).

14. *See infra* notes 113–156 and accompanying text.

15. *See infra* Section IV.C.

16. Clay Johnson, *Hillary's Email*, MEDIUM (Mar. 3, 2015), https://medium.com/@cjoh/hillary-s-email-858ccfc48277#.ka72t7uwj.

If the status quo remains, inadequate regulation will continue to hamstring government transparency and record keeping. This Note analyzes the current regulatory scheme and proposes a solution to ensure more exacting email retention and secure email regulation. Part I explores the purposes of transparency laws. Part II outlines the laws currently governing creation, retention, and disclosure of government records—with an emphasis on email records. Part III explains how the current email retention framework fails to address the security and conflict-of-interest issues present and is thus inadequate. Finally, Part IV proposes a two-pronged solution: a ban on private email use for government business and increased government spending for IT.

I. PURPOSES OF TRANSPARENCY LAWS

Government transparency laws rest on the principle that citizens should have access to information regarding their government's activities.[17] Many rationales have been offered to justify transparency laws. Among them are the public's interest in monitoring government actors, providing input and feedback to government entities, and having a complete documentary record of governmental activity.[18]

One central purpose of government-transparency laws is to facilitate public access to government information.[19] An informed citizenry has long been thought of as a check on excessive executive power.[20] In theory, transparency allows the public to "monitor government activity and hold officials, particularly incompetent and corrupt ones, accountable for their actions."[21] Transparency may also improve governance by facilitating review of and input on government actions by the public at large.[22]

Another important reason for government record keeping is the informational value of documenting government transactions, policies,

17. WENDY GINSBERG ET AL., CONG. RESEARCH SERV., R42817, GOVERNMENT TRANSPARENCY AND SECRECY: AN EXAMINATION OF MEANING AND ITS USE IN THE EXECUTIVE BRANCH 1–2 (2012), https://www.fas.org/sgp/crs/secrecy/R42817.pdf.

18. Mark Fenster, *The Opacity of Transparency*, 91 IOWA L. REV. 885, 899–900 (2006).

19. *About FOIA*, U.S. DEP'T JUST., http://www.justice.gov/open/foia (last updated Nov. 20, 2014).

20. *See, e.g.*, N.Y. Times Co. v. United States, 403 U.S. 713, 728 (1971) (Stewart, J., concurring). *But see* Mark Fenster, *Transparency in Search of a Theory*, 18 EUR. J. SOC. THEORY 150 (2015) (arguing that the theory and assumptions underlying transparency's benefits are flawed).

21. Fenster, *supra* note 18, at 899.

22. *Id.* at 900.

procedures, operations, and so on.[23] Preserved historical records can thus be examined and later used to understand past and present governmental operations.[24]

The passage of the Freedom of Information Act (FOIA)[25] capped off a decade-long movement to enact legislation vesting private citizens with access to government information.[26] The FOIA's enactment came despite consistent executive branch opposition.[27] This conflict illustrates the tension between transparency objectives and legitimate security concerns that follow the opening of the government's files to the public.

II. STATUTORY FRAMEWORK

This Note focuses on the three transparency statutes regulating government agencies and officials: the FOIA, the Federal Records Act (FRA),[28] and the Presidential Records Act (PRA).[29] These statutes can be understood as serving different and exclusive functions—regulating the creation and retention of records on the one hand and regulating their disclosure on the other.[30] While the FOIA regulates disclosure practices,[31] it sets no record-keeping standards.[32] Instead, the FRA and PRA govern record-keeping practices, with each covering different types

23. WENDY GINSBERG, CONG. RESEARCH SERV., R43072, COMMON QUESTIONS ABOUT FEDERAL RECORDS AND RELATED AGENCY REQUIREMENTS 2, 5 (2015), http://www.fas.org/sgp/crs/secrecy/R43072.pdf.

24. WENDY GINSBERG, CONG. RESEARCH SERV., R40238, THE PRESIDENTIAL RECORDS ACT: BACKGROUND AND RECENT ISSUES FOR CONGRESS 1 (2014), https://www.fas.org/sgp/crs/secrecy/R40238.pdf.

25. Pub. L. No. 89-554, 80 Stat. 383 (1966) (codified as amended at 5 U.S.C. § 552 (2012)).

26. *See* Thomas Blanton, *Freedom of Information at 40*, NAT'L SECURITY ARCHIVE (July 4, 2006), http://nsarchive.gwu.edu/NSAEBB/NSAEBB194/index.htm.

27. *See id.* When President Johnson signed the FOIA, he preemptively called for measured use of the law with a signing statement cautioning against disclosure of military secrets and investigative files, among other things. Statement by the President Upon Signing the "Freedom of Information Act," 1 PUB. PAPERS 316 (July 4, 1966). Executive officials were not the FOIA's only critics; then-Professor Antonin Scalia forcefully argued that the FOIA is fundamentally flawed and that its costs vastly outweigh its benefits. *See* Antonin Scalia, *The Freedom of Information Act Has No Clothes*, REGULATION, Mar./Apr. 1982, at 14, 16–19.

28. Federal Records Act of 1950, Pub. L. No. 81-849, 64 Stat. 583 (codified as amended in scattered sections of 44 U.S.C.).

29. Presidential Records Act of 1978, Pub. L. No. 95-591, 92 Stat. 2523 (codified as amended at 44 U.S.C. §§ 2201–09).

30. Armstrong v. Bush, 721 F. Supp. 343, 345 (D.D.C. 1989), *rev'd in part on other grounds*, 924 F.2d 282 (D.C. Cir. 1991).

31. *See* Kissinger v. Reporters Comm. for Freedom of the Press, 445 U.S. 136, 150 (1980) (explaining that the FOIA ensures private access to certain government records).

32. *See Armstrong*, 721 F. Supp. at 345 ("FOIA . . . is a disclosure statute, and a disclosure statute only; it imposes no obligations and provides no guidance for the creation or disposal of particular records.").

of records created by different entities.[33] Material governed by the FRA and PRA is subject to the disclosure mechanisms of the FOIA.[34]

A. *Record Disclosure: Freedom of Information Act*

At its most basic level, the FOIA vests the public with the "right to access information from the federal government."[35] The FOIA was only necessary because the U.S. Supreme Court has consistently rejected the notion that the First Amendment guarantees citizens a right to access government information.[36] In the absence of a constitutional right of private citizens to access government information, the FOIA has supplied that right.[37]

The FOIA's legislative history is replete with references to Congress's desire to vindicate the public right to access information.[38] And although the Supreme Court has recognized a right to *receive* information,[39] it has "relied on FOIA, not the Constitution, to protect *access* to other government information."[40] The FOIA thus serves as the primary vehicle enabling the public to obtain information sought from the government.[41]

Section (a) of the FOIA generally requires that agencies make certain information available to the public[42] and disclose records in response to requests.[43] Section (b) enumerates nine classes of information exempt from disclosure and provides procedures for redacting exempted material from documents capable of partial disclosure.[44] The exemptions protect

33. The FRA applies to "each Federal agency." 44 U.S.C. § 3101 (2012). "[T]he term 'Federal agency' means any executive agency or any establishment in the legislative or judicial branch of the Government" and does not mean the Supreme Court, Congress, or Architect of the Capitol. *Id.* § 2901(14). The PRA, however, regulates "Presidential records," defined as "documentary materials, or any reasonably segregable portion thereof, created or received by the President, [the President's] immediate staff," or someone advising or assisting the President. *Id.* § 2201(2).

34. *See* 5 U.S.C. §§ 552(a)(3), (f)(1).

35. *See What is FOIA?*, FOIA.GOV, http://www.foia.gov/ (last visited Sept. 30 , 2016).

36. *See, e.g.*, McBurney v. Young, 133 S. Ct. 1709, 1718 (2013) ("This Court has repeatedly made clear that there is no constitutional right to obtain all the information provided by FOIA laws."); Houchins v. KQED, Inc., 438 U.S. 1, 14–15 (1978) ("Neither the First Amendment nor the Fourteenth Amendment mandates a right of access to government information or sources of information within the government's control.").

37. *See* Barry Sullivan, *FOIA and the First Amendment: Representative Democracy and the People's Elusive "Right to Know,"* 72 MD. L. REV. 1, 17–18 (2012).

38. *See* S. REP. NO. 89-813, at 37–38 (1965).

39. *See* Martin v. Struthers, 319 U.S. 141, 143 (1943).

40. Susan Nevelow Mart, *Let the People Know the Facts: Can Government Information Removed from the Internet Be Reclaimed?*, 98 LAW LIBR. J. 7, 9 (2006).

41. *See* Sullivan, *supra* note 37, at 66.

42. 5 U.S.C. § 552(a)(1)–(2) (2012).

43. *Id.* § 552(a)(3).

44. *Id.* § 552(b).

from disclosure records containing, for example, classified information, trade secrets, and personal information.[45] The FOIA grants district courts authority to enjoin government agencies "from withholding agency records" and to order the production of improperly withheld records.[46]

The FOIA applies to "government agencies," defined as any department, government corporation, or other creation of the executive branch.[47] Unlike the term "government agency," the FOIA does not define "record," although it makes clear that the FOIA covers electronically stored information that would otherwise be a record.[48]

The Supreme Court has borrowed the definition of "agency record" from other statutes to determine what records the FOIA covers.[49] Records can thus be described as "documentary materials . . . *made or received* by an agency of the United States Government under Federal law or in connection with the transaction of public business."[50]

Additionally, to be subject to the FOIA, requested materials must be in the possession of the agency when the request is made.[51] This possession requirement was the subject of the landmark Supreme Court case *Kissinger v. Reporters Committee for Freedom of the Press*.[52] The Court in *Kissinger* held that courts may only intervene when "an agency has (1) 'improperly'; (2) 'withheld'; (3) 'agency records.'"[53] When an agency record is removed from the agency's possession before a FOIA request, the agency lacks the possession necessary to withhold the record.[54] This means that records removed from an agency's control are beyond FOIA's grasp. This possession requirement evinces FOIA's narrow focus of providing access to records rather than directing their creation or maintenance.[55]

---

45. *Id.*

46. *Id.* § 552(a)(4)(B).

47. *Id.* §§ 551(a), 552(f)(1). The FOIA regulations do not govern Congress, the courts, and several other bodies. *Id.* § 551(a).

48. *Id.* § 552(f)(2)(A).

49. U.S. Dep't of Justice v. Tax Analysts, 492 U.S. 136, 145 (1989); Forsham v. Harris, 445 U.S. 169, 183 (1980).

50. *Forsham*, 445 U.S. at 183 (emphasis added) (quoting 44 U.S.C. § 3301).

51. *See Tax Analysts*, 492 U.S. at 145 ("[T]he agency must be in control of the requested materials at the time the FOIA request is made. By control we mean that the materials have come into the agency's possession in the legitimate conduct of its official duties.").

52. 445 U.S. 136, 152 (1980) ("The [FOIA] does not obligate agencies to create or retain documents; it only obligates them to provide access to those which it in fact has created and retained.").

53. *Id.* at 150 (quoting 5 U.S.C. § 552(a)(4)(B)).

54. *Id.* at 150–51.

55. *Id.* at 152.

B. *Record Retention*

Despite its foundational importance, the FOIA is not without its limitations. Its reach is limited to records within an agency's control.[56] This limitation is, for the most part, mitigated by statutes mandating the preservation of records. The FRA and the PRA are principally concerned with the handling, creation, and preservation of government records and information.[57] These laws bolster the FOIA by ensuring the preservation of records subject to disclosure.[58]

1. Federal Records Act

The FRA governs executive agencies' creation, management, and disposal of records.[59] The FRA facilitates public access to records by ensuring their retention so they may be available for subsequent FOIA requests. After all, "proper records management is the backbone of open Government."[60]

Unlike the FOIA, the FRA explicitly defines "records."[61] The FRA-provided definition of records, like the definition the Supreme Court attributed to the FOIA, is expansive.[62] The 2014 FRA amendment shifted the emphasis away from the medium in which the information was stored to the information itself.[63] Accordingly, the definition of agency record refers "generically to 'recorded information.'"[64] Emails clearly fit this broad category and are thus subject to preservation.[65]

For the purposes of this Note's analysis, the 2014 FRA amendments' treatment of email records is most relevant. Before the amendments, the law required government employees to preserve email records, but it did not require them to preserve the records in an official location—meaning that officials such as Secretary Clinton were free to create and maintain

---

56. *Id.*

57. *See* Armstrong v. Bush, 924 F.2d 282, 284–85 (D.C. Cir. 1991).

58. *See* Armstrong v. Bush, 721 F. Supp. 343, 345 (D.D.C. 1989) ("Several federal statutes combine to ensure the permanent retention and public disclosure of a broad variety of federal 'records.'"), *rev'd in part on other grounds*, 924 F.2d 282 (D.C. Cir. 1991).

59. The "Federal Records Act" refers to four U.S. Code chapters governing federal records: (1) National Archives and Record Administration, 44 U.S.C. §§ 2101–20 (2012); (2) Records Management by the Archivist of the United States, §§ 2901–11; (3) Records Management by Federal Agencies, §§ 3101–07; (4) Disposal of Records, §§ 3301–14.

60. Memorandum on Managing Government Records, 2011 DAILY COMP. PRES. DOC. 1 (Nov. 28, 2011).

61. *See* 44 U.S.C. § 3301.

62. *See id.*; Forsham v. Harris, 445 U.S. 169, 183 (1980).

63. GINSBERG, *supra* note 23, at 2.

64. *Id.*

65. *Id.*

email records entirely on private servers.[66] The amended FRA requires that agency officials copy or forward copies of records created or received on an unofficial email account to an official government email account.[67] Under this subsection, employees are free to conduct official business from private accounts so long as these messages make it to a government email inbox within the allotted time frame.[68]

Government employees are not completely free, however, to send confidential information on private email accounts. A number of laws impose penalties for knowingly or negligently disclosing *classified* material.[69] Indeed, much of the Clinton controversy centered on whether Clinton sent or received classified information on her private server.[70]

The FRA only mandates retention of *records*—non-records need not be forwarded to a government email.[71] For instance, emails relating to professional meetings that do not document agency activity do not constitute records.[72] However, emails relating to both personal matters and government business constitute records.[73] Naturally, these parameters create ambiguity as to which emails government employees must forward.

Federal agency heads are tasked with ensuring FRA compliance.[74] Agency chiefs "shall make and preserve records" documenting the agency's activities and must establish a records-management program.[75] It is their responsibility to safeguard against the improper removal or destruction of records and to report any discovered removal or destruction of records.[76] The FRA provides guidelines for the proper destruction of agency records.[77] Agency records may not be removed or destroyed by other means.[78] Intentional violators who fail to forward records created

66. *See, e.g.*, Brent Kendall, *Hillary Clinton's Personal Email Use Came Before Recent Rule Changes*, WASH. POST (Mar. 3, 2015, 3:40 PM), http://www.wsj.com/articles/hillary-clintons-personal-email-use-came-before-recent-rule-changes-1425415233.

67. *See* 44 U.S.C. § 2911(a).

68. *See id.*

69. *See* 18 U.S.C. §§ 793(f), 1924(a).

70. Elizabeth Goitein, *Five Myths About Classified Information*, WASH. POST (Sept. 18, 2015), https://www.washingtonpost.com/opinions/five-myths-about-classified-information/2015/09/18/a164c1a4-5d72-11e5-b38e-06883aacba64_story.html.

71. *See* 44 U.S.C. § 2911.

72. *See, e.g.*, DEP'T OF HOMELAND SEC. RECORDS MGMT., E-MAIL MANAGEMENT 8, http://www.archives.gov/records-mgmt/toolkit/pdf/ID317.pdf (last visited Oct. 24, 2016).

73. 36 C.F.R. § 1222.20(b)(2) (2015) ("If information about private matters and agency business appears in a received document, the document is a Federal record.").

74. 44 U.S.C. §§ 3101–06.

75. *Id.* §§ 3101–02.

76. *Id.* § 3106.

77. *Id.* §§ 3301–16.

78. Id. § 3314.

or received on a private email account are subject to non-criminal punishment ranging from a week's suspension to firing.[79]

2. Presidential Records Act

The PRA governs the creation, retention, and eventual archival or destruction of records "created or received by the President, [the President's] immediate staff," or other executive individuals working in an official capacity for the executive branch.[80] The PRA and the FRA cover a mutually exclusive set of records but serve the same general function.[81] They each direct covered individuals to preserve certain records created or received while conducting official business and provide for specific disposal procedures.[82]

Critically, the PRA adopts the same procedures as the FRA for preserving records created or received on an unofficial email address[83]: Employees who send or receive an official record on an unofficial email account must either copy or forward the email to an official email account within twenty days.[84] The disciplinary protocol the PRA establishes for violators is identical to that of the FRA.[85]

C. *Relationship Between Disclosure and Retention Statutes*

The FRA and PRA govern the way government agencies and the executive branch collect, preserve, and dispose of federal records.[86] The FOIA, on the other hand, provides a mechanism for accessing executive branch and federal agency records.[87] The FRA and PRA can thus properly be viewed "as ensuring the proper collection and retention" of materials to be later disclosed under the FOIA.[88]

III. PROBLEMS WITH THE PERMISSION PARADIGM

As currently formulated, both the PRA and the FRA permit covered employees to conduct official duties on private email addresses so long as an official email account receives a copy of the record.[89] Thus, covered

79. *Id.* § 2911(b). Even stiffer punishment may be imposed on a person found guilty of "willfully and unlawfully" concealing, removing, or destroying a federal record. 18 U.S.C. § 2071(b). Violators face fines, up to three years imprisonment, or both. *Id.*

80. 44 U.S.C. §§ 2201–09.

81. *Id.* § 2201(2)(B) (noting that the statute does not cover "official records of an agency").

82. Armstrong v. Bush, 924 F.2d 282, 284–86 (D.C. Cir. 1991).

83. 44 U.S.C. §§ 2209, 2911.

84. *Id.* § 2209.

85. *Id.* §§ 2209(b), 2911(b).

86. *See supra* Section II.B.

87. *See supra* Section II.A.

88. GINSBERG, *supra* note 23, at 11.

89. 44 U.S.C. §§ 2209(b), 2911(b).

officials retain discretion as to when private emails contain subject matter that requires retention. This formulation creates perverse incentives for government employees and is fraught with security risks. This Part will analyze some of the inherent problems of a permission-with-regulation regime.

A. *Rule Breaking*

Letting a government employee decide which emails to retain creates a conflict of interest. The public has an interest in the most disclosure practicable, while government employees have an interest in disclosure that will not be personally damaging. The public and the government employees' record-keeping goals are therefore at odds.

1. A Useful Analogy: The Classification System

An illustrative example of government employees' anti-disclosure posture is the classification system. The classification system exists to prevent disclosure of sensitive information that could injure national security.[90] It generally consists of rules and procedures that guide the protection of government records containing sensitive or confidential information.[91] Despite the straightforward mandate of information classification,[92] it has long been recognized that the classification system conceals a great deal of documents that could hardly be characterized as injurious to national security if disclosed.[93] For instance, intelligence agencies labeled as "top secret" an email sent to Hillary Clinton that included discussion on a "widely known and discussed" drone strike.[94]

---

90. Exec. Order No. 13,526, 3 C.F.R. 298 (2010), *reprinted in* 50 U.S.C. § 435 (2012).

91. *Id.*

92. *Id.*

93. *See* Steven Aftergood, *Reducing Government Secrecy: Finding What Works*, 27 YALE L. & POL'Y REV. 399, 402–04 (2009); Jeffrey Toobin, *Hillary's Problem: The Government Classifies Everything*, NEW YORKER (Aug. 18, 2015), http://www.newyorker.com/news/daily-comment/hillarys-problem-the-government-classifies-everything. In a 2010 hearing, National Security Archive Director Thomas Blanton estimated that approximately fifty to ninety percent of classified material should not be classified. *Hearing on the Espionage Act and the Legal and Constitutional Implications of Wikileaks: Hearing Before the H. Comm. on the Judiciary*, 111th Cong. 160 (2010) (statement of Thomas Blanton, Director, National Security Archive), http://nsarchive.gwu.edu/news/20101216/Blanton101216.pdf.

94. Bradley Klapper & Ken Dilanian, *AP EXCLUSIVE: Top Secret Clinton Emails Include Drone Talk*, AP: BIG STORY (Aug. 14, 2015, 9:32 PM), http://bigstory.ap.org/article/b54a250a40e9410baaaca5f9fb58ea94/ap-exclusive-top-secret-clinton-emails-include-drone-talk ("Neither of the two emails sent to Hillary Rodham Clinton now labeled by intelligence agencies as 'top secret' contained information that would jump out to experts as particularly sensitive, according to several government officials.").

For decades, commentators have lamented abuses of the classification system and "excessive government secrecy."[95] Numerous task forces, commissions, and committees have diagnosed government over-classification as a problem and suggested solutions.[96] Few of these initiatives, however, have significantly reduced the excesses of government classification.[97] In 2014, executive agencies completed over seventy-seven million classification actions.[98]

The properties and structure of the classification system can partly account for the over-classification problem. Critically, more than four million government officials have authority to classify documents.[99] Further, the categories under which government employees may classify documents are so vague as to cover a broad range of documents that would have no bearing on national security if released.[100] These reasons alone, however, do not evince a clear rationale for why government employees consistently err on the side of over-classification rather than under-classification.[101]

Principal reasons for consistent over-classification have more to do with the interests and motivations of the individuals participating in the classification system than the structure of the system itself. One recent article pointed to "bureaucratic secrecy"[102] and "political secrecy"[103] as drivers of improper classification practices. Accounting for these interests, over-classification has little to do with national security.[104] Instead, some of the most prevalent factors include suspicion that disclosure is inherently riskier than non-disclosure, convenience, desires to avoid controversy and accountability, and political expediency.[105]

---

95. Aftergood, *supra* note 93, at 404.

96. *Id.* at 404–06.

97. *See id.*

98. INFO. SEC. OVERSIGHT OFFICE, 2014 REPORT TO THE PRESIDENT 5 (2014), http://www.archives.gov/isoo/reports/2014-annual-report.pdf. Maintaining the classification system cost roughly $14.98 billion in 2014. *Id.* at 24.

99. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, 2014 REPORT ON SECURITY CLEARANCE DETERMINATIONS 5 tbl.1.3 (2015); Goitein, *supra* note 70.

100. Fenster, *supra* note 18, at 923 (noting the ease of fitting a "document's information within one of the broad and vague categories provided by the Executive Order establishing the classification system").

101. *Id.* at 923–24 ("Tellingly, the inadvertent release of classified documents is far rarer than the inadvertent classification of information that does not warrant protection.").

102. Aftergood, *supra* note 93, at 402 (noting the "tendency of bureaucracies . . . to hoard information").

103. *Id.* at 403 ("[Political secrecy] exploits the generally accepted legitimacy of genuine national security interests in order to advance a self-serving agenda, to evade controversy, or to thwart accountability.").

104. *See* Goitein, *supra* note 70.

105. *See* Aftergood, *supra* note 93, at 402–03; Fenster, *supra* note 18, at 923.

Taken together, classification policies and inherently biased classifiers have produced a mass of uncertainty and excessive government secrecy.

The Interagency Security Classification Appeals Panel (ISCAP)[106] example illustrates these classification tendencies. Created by executive order in 1995, the ISCAP is comprised of senior-level representatives of the Departments of State, Defense, and Justice, the Central Intelligence Agency, the National Archives, and the National Security Council.[107] The Panel adjudicates appeals of agency decisions denying declassification requests.[108] Between 1996 and 2014, the Panel declassified some or all of the requested documents in 1,387 of 1,960 appeals heard.[109] To put this in context, federal courts, which generally defer to executive decisions, hear similar appeals but "almost never overturn agency classification decisions."[110]

Reconciling the success of the Panel with the fact that its members are the very organizations whose decisions are being questioned requires analysis of the Panel members' interests. While political and bureaucratic secrecy drive over-classification within agencies, those unique organizational interests are not persuasive to the Panel as a whole.[111] Instead, the Panel members' joint interest in national security guides decisions whether to declassify, and the Panel overturns classification decisions based on illegitimate factors.[112]

It is likely that the factors contributing to over-classification of government records would similarly cause abuses of the FRA and the PRA's guidelines for private email retention. As a preliminary matter, the government employees making classification decisions are the same individuals governed by records-retention laws. They are demonstrably risk-averse and generally err on the side of self-preservation through over-classification.[113] Thus, a government employee who classifies records unnecessarily in the interest of self-preservation would likely neglect to forward potentially damaging emails sent or received on a private email address even if the email was an official record. That is, a government employee forced to choose[114] whether an email is an official

106. Exec. Order No. 12,958, 3 C.F.R. 333, 352–53 (1996), *reprinted as amended in* 50 U.S.C. § 435 (2012).

107. *Id.* The represented agencies are among "the most prolific classifiers." Aftergood, *supra* note 93, at 407.

108. Exec. Order No. 13,526, 3 C.F.R. 298, 319–20 (2010), *reprinted in* 50 U.S.C. § 435.

109. INFO. SEC. OVERSIGHT OFFICE, *supra* note 98, at 22.

110. Aftergood, *supra* note 93, at 407 (noting that courts have overturned agency classification decisions in "no more than a few dozen FOIA cases over the past thirty years").

111. *Id.* at 408–09.

112. *Id.*

113. *See id.* at 402–03; Fenster, *supra* note 18, at 923.

114. *See supra* notes 67–73 and accompanying text.

record would more often than not neglect to preserve it on an official email account, regardless of whether it is actually an official record.[115] Without modification to the law, such individuals will retain only emails that pose no threat to their interests.

It should be noted, however, that this is an imperfect analogy. Over-classification is a problem, but the generous classification decisions themselves are not illegal because of the vague classification categories that make the system susceptible to abuse.[116] On the other hand, failing to copy or forward potentially damaging emails covered by the PRA or the FRA to an official email account is illegal.[117] This distinction between rule bending and rule breaking is important to note in predicting the observance of the current email-retention scheme. However, the same interests remain prevalent and would likely cause a significant number of emails to elude preservation.

2. Classification's Impact on Email

Government email regulation is more than just analogous to the classification system—the two systems are highly intertwined. Agency rules mandate that government employees must transmit classified information only via classified networks.[118] Sending classified information on a network the agency has not approved to handle classified messages may result in criminal sanctions or a security violation.[119]

Given the documented abuse of the classification system, the government's stance against transmission of classified information on unsecure networks is at odds with its current allowance for official emails on private accounts. The Clinton email controversy speaks directly to this issue. Ever since Clinton's emails were made public, the State Department has engaged in a public disagreement with intelligence agencies and Congress over whether and when the emails on Clinton's server were classified.[120] This disagreement begs the question: If government agencies cannot agree on what information belongs on a

115. *See* Aftergood, *supra* note 93, at 402–04; Fenster, *supra* note 18, at 923.

116. *See* Fenster, *supra* note 18, at 923.

117. 44 U.S.C. §§ 2209(b), 2911(b) (2012).

118. *See, e.g.*, Dep't of the Army, Regulation 380-5, Information Security Program § 8, at 90–91 (Sept. 29, 2000), https://fas.org/irp/doddir/army/ar380-5.pdf.

119. *See id.*; *supra* note 4.

120. *See* Eric Lichtblau & Stevn Lee Myers, *Agencies Clashed on Classification of Clinton Email, Inquiry Shows*, N.Y. TIMES (Oct. 17, 2016), http://www.nytimes.com/2016/10/18/us/politics/hillary-clinton-emails-fbi.html; Steven Lee Myers & Mark Mazzetti, *Agencies Battle over What Is 'Top Secret' in Hillary Clinton's Emails*, N.Y.TIMES (Feb. 5, 2016), http://www.nytimes.com/2016/02/06/us/politics/agencies-battle-over-what-is-top-secret-in-hillary-clintons-emails.html.

secure government server, is it reasonable to expect individual government employees to make this determination correctly?

Because the classification system involves a great deal of uncertainty as to what is and is not classified, email regulations should not distinguish between classified and unclassified content. Allowing official emails on private email accounts creates additional uncertainty and renders government employees vulnerable to allegations of mishandling classified information because of flexible classification parameters.[121]

3. Undermining the Objectives of Transparency Laws

Non-compliance with the PRA and the FRA's email guidelines prevents those statutes from achieving their purpose. The public cannot effectively monitor the government when many government emails can easily be kept out of reach.[122] An incomplete record limits public review and criticism of government activities and reduces the "informational value" of available government documents.[123] Since governmental entities do not possess records that government employees fail to copy to an official email address, the FOIA would be circumvented as to the unforwarded records.[124]

While the classification system doubtless serves an important function, excessive use of classification hinders the objectives advanced by transparency laws.[125] And just as an agency official with classification authority can shield information from public scrutiny, any government official who transacts official business on a private email address can similarly keep the substance of his emails secret by neglecting to forward.[126]

However, even when a government official complies with the PRA and the FRA's email mandates by copying official emails to government email addresses,[127] accessing these emails after the fact may be impractical if they are not all forwarded to the same email address.[128] FOIA requests often require officials to search thousands of records to

---

121. *See* Fenster, *supra* note 18, at 923; Toobin, *supra* note 93.

122. *See supra* Part I.

123. *See id.*

124. *See supra* Section II.A.

125. Alexander M. Taber, Note, *Information Control: Making Secrets and Keeping Them Safe*, 57 ARIZ. L. REV. 581, 594–95 (2015).

126. *See supra* Section III.A.

127. 44 U.S.C. §§ 2209(a), 2911(a) (2012).

128. *See, e.g.*, NAT'L ARCHIVES & RECORDS ADMIN., NARA BULL. NO. 2011-03, GUIDANCE CONCERNING THE USE OF E-MAIL ARCHIVING APPLICATIONS TO STORE E-MAIL (2010), http://www.archives.gov/records-mgmt/bulletins/2011/2011-03.html (requiring email record-keeping systems that facilitate the "grouping of related records" and "[p]ermit easy and timely retrieval" of records).

find responsive documents,[129] and when the email records are preserved in tens or hundreds of different email inboxes, fulfilling a FOIA request becomes impractical.[130] Therefore, even compliance with records-retention statutes may circumvent the FOIA.

B. *Security*

Allowing government employees to conduct official business from private email accounts on private servers results in inconsistent—and probably insufficient—security of potentially sensitive information. The prevalence of hacking has created an environment where digital information is less secure than ever. In such a threat-ridden online world, allowing individual employees to take email security into their own hands is a risky endeavor.

Hackers and other nefarious parties threaten the confidentiality, integrity, and availability of email—the primary form of communication for many.[131] Some of the most significant recent hacks originated via email.[132] Two notable tactics hackers use to perpetrate cyber attacks are spear phishing and social engineering. Spear phishing is the process by which hackers send seemingly personal emails to their target utilizing publicly available personal information in a bid to convince the target to disclose valuable information.[133] In the hacking context, social engineering is "the art of manipulating people so they give up confidential information."[134]

---

129. *See What Is the Freedom of Information Act (FOIA) and Why Should You Care?*, NAT'L TRANSP. SAFETY BOARD, http://www.ntsb.gov/about/foia/Pages/freedom_and_information.aspx (last visited Oct. 24, 2016).

130. Lauren Carroll, *Hillary Clinton's Email: Did She Follow All the Rules?*, POLITIFACT (Mar. 12, 2015, 3:16 PM), http://www.politifact.com/truth-o-meter/article/2015/mar/12/hillary-clintons-email-did-she-follow-all-rules/.

131. PAM COCCA, SANS INST., EMAIL SECURITY THREATS 3 (2005), https://www.sans.org/reading-room/whitepapers/email/email-security-threats-1540; RADICATI GRP., INC., US EMAIL STATISTICS REPORT, 2016-2020, at 2–3 (2016), http://www.radicati.com/wp/wp-content/uploads/2016/03/US-Email-Statistics-Report-2016-2020-Executive-Summary.pdf.

132. *See* Richard Chirgwin, *Ubiquiti Stung US$46.7 Million in E-mail Spoofing Fraud*, THE REGISTER (Aug. 9, 2015, 10:44 PM), http://www.theregister.co.uk/2015/08/09/ubiquiti_stung_by_email_spoofing_fraud/; Gerry Smith, *Massive Target Hack Traced Back to Phishing Email*, HUFFPOST BUS. (Feb. 12, 2014, 3:56 PM), http://www.huffingtonpost.com/2014/02/12/target-hack_n_4775640.html.

133. *Spear Phishers Angling to Steal Your Financial Info*, FED. BUREAU INVESTIGATION (Apr. 1, 2009), https://www.fbi.gov/news/stories/2009/april/spearphishing_040109.

134. *Social Engineering: A Hacking Story*, INFOSEC INST. (Sept. 23, 2013), http://resources.infosecinstitute.com/social-engineering-a-hacking-story/. Social engineering attacks can target individuals or service providers. For the purposes of this Note, attacks against service providers are most relevant because attacks seeking information directly from the targeted individual are possible regardless of the entity servicing the email account.

While serving as Secretary of State, Hillary Clinton's private email was reportedly subjected to at least five phishing attempts.[135] The attacks were apparently not successful, but they underscore the risk that a careless click could have caused a leak of sensitive information.[136] Some have suggested that Clinton's email setup was especially vulnerable to hacks because it was independently maintained by Clinton and her staff and unprotected by State Department security staff—or even by security measures offered by private email providers like Microsoft or Yahoo.[137]

Email accounts maintained on independent servers are not the only accounts at risk. Personal email accounts hosted by Internet companies are also targeted. The recent hack of CIA Director John O. Brennan's private email account provides an example of the risks created when government officials conduct business on a personal email account hosted by Internet companies.[138] In a recent address to the Council on Foreign Relations, Brennan touted the CIA's efforts to improve cyber defenses.[139] Yet, months later, a hacker—allegedly a high school student—breached Brennan's personal email account[140] and went on to release sensitive documents that Brennan had in his personal email account's inbox.[141] The hacker claims to have used "social engineering" to pose as Brennan and acquire his personal information and email credentials from Verizon and AOL.[142] The hack on Brennan's AOL

---

135. Bradley Klapper et al., *Emails: Russia-Linked Hackers Tried to Access Clinton Server*, AP: BIG STORY (Oct. 1, 2015, 2:51 AM), http://bigstory.ap.org/article/9160a25f39e14507ab90c977d300dc8b/6000-more-pages-clinton-emails-be-published-wednesday. The malicious emails were disguised as speeding tickets from New York Department of Motor Vehicles. *Id.* Downloading the "attachment would have allowed hackers to take over control of [Clinton's] computer." *Id.*

136. *See id.*

137. Andy Greenberg, *Why Clinton's Private Email Server Was Such a Security Fail*, WIRED (Mar. 4, 2015, 5:32 PM), http://www.wired.com/2015/03/clintons-email-server-vulnerable/.

138. Phillip Messing et al., *Teen Says He Hacked CIA Director's AOL Account*, N.Y. POST (Oct. 18, 2015, 11:40 PM), http://nypost.com/2015/10/18/stoner-high-school-student-says-he-hacked-the-cia/.

139. *Director Brennan Speaks at the Council on Foreign Relations*, CENT. INTELLIGENCE AGENCY (Mar. 13, 2015), https://www.cia.gov/news-information/speeches-testimony/2015-speeches-testimony/director-brennan-speaks-at-the-council-on-foreign-relations.html.

140. Messing et al., *supra* note 138.

141. Damian Paletta, *CIA Director's Personal Email Allegedly Hacked*, WALL ST. J. (Oct. 19, 2015, 5:35 PM), http://www.wsj.com/articles/cia-directors-personal-email-allegedly-hacked-1445290540. The hacker released a contact list containing 2,611 email and instant-message addresses, including contacts of CIA employees and top intelligence officials. *Id.* The hacker also accessed Brennan's application for top-secret security clearance, among other sensitive files. *Id.*

142. Kim Zetter, *Teen Who Hacked CIA Director's Email Tells How He Did It*, WIRED (Oct. 19, 2015, 6:14 PM), http://www.wired.com/2015/10/hacker-who-broke-into-cia-director-john-brennan-email-tells-how-he-did-it/.

account showed that even those individuals who are keenly aware of the dangers posed by cyber threats are nonetheless susceptible to attacks when they use personal email accounts.

As long as government officials transmit valuable information online, malicious actors will seek to steal it. This eminent threat requires that digital messages be protected with the most secure systems available. The types of attacks faced by Clinton's and Brennan's personal email accounts are commonplace today.[143] Allowing government officials to transmit official government records on private email accounts has the obvious effect of putting these records at unnecessary risk.

IV. A SOLUTION: PROHIBITION

This Note argues that the best way to solve the security and conflict-of-interest problems discussed above is to prohibit government officials from conducting official business on private email accounts. This prohibition will limit their ability to sidestep records-retention laws, thereby advancing transparency laws' objectives. Further, sensitive information contained in official records would be more secure on official email accounts. This ban is also necessary to prevent rampant violations of regulations governing classified information. This solution, of course, is not perfect, as some rule breaking and security breaches are inevitable; however, prohibiting the use of private email accounts will significantly improve record preservation and security.

To facilitate the prohibition of official business on private email addresses, government IT capabilities must also be improved. Substantial investment in IT would serve to enhance the security and convenience of using government email accounts.

A. *Reducing Rule Breaking*

Prohibiting the use of private email accounts for official business would minimize the risk of rule breaking that is all too likely under the current permission-with-regulation paradigm.[144] This Note's solution would modify the incentives of retention-law compliance by raising the cost of non-compliance and making compliance a more attractive option. Further, policing prohibition would be more straightforward than policing a permission-with-regulation scheme. Finally, this Note's solution will induce officials who nonetheless break the rules and conduct official business on private email accounts to break the rules to a lesser extent.

---

143. *Cyber Crime*, FBI.gov, https://www.fbi.gov/investigate/cyber (last visited Sept. 30, 2016).

144. *See supra* Section III.A.

1. Balancing Incentives

Basic economic principles illustrate why prohibition would deter government officials from using private email accounts for official business. Legal economists generally view decisions to engage in criminal behavior as rational decisions made by individuals who expect the benefit of the activity to exceed the cost.[145] Thus, criminal behavior may be reduced by increasing the *cost* of the behavior to a level exceeding the benefit—ensuring that crime does not *pay*.

Basic economic theory presupposes that individuals are rational and self-interested.[146] Put simply, considerations of costs and benefits guide—either implicitly or explicitly—the choices people make.[147] Accordingly, researchers have observed that individuals generally engage in more of an activity when the perceived benefits increase and engage in less of an activity when the perceived costs increase.[148]

Criminal law utilizes these same principles to eliminate socially undesirable activities by making the commission of crimes more costly.[149] Two factors relevant to an individual's decision whether to engage in criminal behavior are the probability of prosecution and the severity of punishment.[150] Accounting for these factors, two options emerge that would appear to reduce the undesirable conduct: (1) increasing the probability of prosecution, and (2) increasing the penalties levied against offenders.[151]

Of the available options, increasing the probability of prosecution would likely have the most significant effect on reducing the undesirable activity—here, transmission of official government emails on private accounts. Studies suggest that probability of enforcement has a far greater deterrent effect than severity of punishment.[152] The deterrent effect of increasing penalties diminishes "rapidly" as the probability of

145. RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 219 (6th ed. 2003). While transmitting official government emails on a private email account is not *currently* illegal, adopting this Note's proposed solution to consider such conduct illegal would substantially reduce levels of rule breaking.

146. JEFFREY L. HARRISON, LAW AND ECONOMICS 54–55 (2007).

147. POSNER, *supra* note 145, at 219.

148. *Id.* at 220; Isaac Ehrlich, *Crime, Punishment, and the Market for Offenses*, 10 J. ECON. PERSPECTIVES 43, 55 (1996).

149. POSNER, *supra* note 145, at 219–20.

150. *Id.*

151. *See id.* at 220–21. To be sure, opportunity costs also affect an individual's behavior. *Id.* at 220. Raising the costs of transmitting official emails on a private server would make alternatives like phone calls and in-person meetings a more desirable alternative for individuals seeking to avoid the message's disclosure. *See* Fenster, *supra* note 18, at 922.

152. Edward K. Cheng, *Structural Laws and the Puzzle of Regulating Behavior*, 100 NW. U. L. REV. 655, 660 (2006).

enforcement falls.[153] Increasing the probability of enforcement also facilitates a more accurate perception of the costs and benefits of a crime, such that would-be criminals are less likely to over- or underestimate the risks of criminal activity.[154]

With these principles in mind, it should be obvious that materially limiting the use of private email accounts for government business must involve more than an increase in penalties—though some level of penalty increase would probably be beneficial. However, any attempt to improve email-record retention should seek to facilitate detection and make enforcement of the rule more likely.

In addition to making rule breaking more costly by raising the likelihood of detection and penalties, stigma effects of punishment could further reduce the utility of improper email use.[155] In the context of high-ranking government officials, the Hillary Clinton event should serve as a strong incentive to keep official emails on government servers. However, the same incentive is weaker—at least relative to that of higher ranking officials—for low- and mid-level government employees who lack political capital but are nonetheless subject to records-retention laws. Nonetheless, criminalizing the activity would raise the costs of the undesired activity and incentivize compliance with records-retention laws.

This Note suggests implementing the prohibition of official emails on private accounts by removing the provisions that shield government employees from liability if they copy or forward the message to an official account.[156] Penalty for violation would be the same as is currently contemplated for failure to copy or forward official emails on private accounts.[157]

The current incentives for officials to use an official government email account are low,[158] and disobeying the rules is pervasive[159] and relatively risk-free.[160] Penalizing the transmission of official emails on private

153. *Id.*

154. POSNER, *supra* note 145, at 227.

155. HARRISON, *supra* note 146, at 243.

156. For the FRA, this would mean eliminating 44 U.S.C. § 2911(a)(1)–(2), while leaving subsection (a) intact before the word "unless." For the PRA, the change would be the same, but § 2209(a) would be affected. These modified provisions would attach liability to senders of official emails from private email accounts. Of course, liability would be inappropriate for the official that receives an unsolicited official email on a private account.

157. 44 U.S.C. §§ 2209(b), 2911(b) (2012).

158. *See, e.g.*, Johnson, *supra* note 16 (arguing that private email servers are more secure and efficient than government servers).

159. *See* sources cited *supra* note 9.

160. Hillary Clinton's private email setup may have never been noticed were it not for a special congressional investigation that failed to uncover any of Clinton's emails from the State

accounts is needed to curtail the rampant rule breaking and create more meaningful transparency.

2. Simplifying Enforcement

Policing a prohibition scheme is more manageable than policing a permission-with-regulation scheme and would better enable detection of violations. First, evidence that a government official failed to use—or barely used—an official email address almost certainly establishes a rule violation. Proof of an email pertaining to government business sent on a private email address would similarly establish a rule violation without inquiry into whether the government employee copied or forwarded the email within an allotted time frame.[161] Mandating official business be conducted on official instead of private email accounts would create a presumption among officials that any email involving government business transmitted on a private email account violates the law.

Policing rule violations under the current rules is much more difficult. As previously discussed, many emails are likely to go unforwarded and would thus be impervious to oversight.[162] These records, which do not end up under government control, are beyond the FOIA's reach.[163] Even records forwarded to an official government email account in accordance with the rules may be difficult to track down if they are scattered among many different inboxes.[164] This Note's solution can overcome these challenges by consolidating email records and bringing them under government control.[165]

Of course, it would be impossible to capture every government communication for later public scrutiny. It has long been recognized that government actors who prefer secrecy will adapt communication mediums to protect information from disclosure.[166] For instance, a

---

Department. Josh Voorhees, *A Crystal-Clear Explanation of Hillary's Confusing Email Scandal*, SLATE (Aug. 20, 2015, 8:15 PM), http://www.slate.com/blogs/the_slatest/2015/08/20/hillary_clinton_email_scandal_explained.html. Since the Clinton email revelation, there have been more discoveries of government employees using private email, and reports indicate that a substantial proportion of government employees still use personal email for business and fail to preserve such emails with little repercussions. Attkisson, *supra* note 9.

161. *See supra* notes 156–57 and accompanying text. However, the limited exception prescribed below would provide immunity in narrowly defined circumstances. *See infra* note 171.

162. *See supra* Section III.A.

163. *See supra* notes 51–55 and accompanying text.

164. *See supra* notes 127–30 and accompanying text.

165. *See supra* Subsection IV.A.1.

166. Fenster, *supra* note 18, at 922, 924 ("When an agency or an individual government official prefers to protect information from disclosure, then the agency or official is more likely to produce it in a form, circulate it by a method, and/or maintain or destroy it so that the information will either fall outside disclosure requirements or avoid detection.").

government official who prefers secrecy may choose to communicate telephonically if he perceives an email would involve a high risk of disclosure.[167] Simply put, perfect information regulation is not possible, and at some level, disclosure avoidance is inevitable.[168] However, prohibiting official business on private email addresses would make enforcement more likely, thus increasing the cost of non-compliance.

3. Shrinking the Exception to the General Rule

Any modification to records-retention statutes must provide for the reality that access to official email accounts may be impractical at times. A server being down[169] and a late-night crisis requiring an immediate response[170] are instances in which transmitting government business on a private email address would be warranted. Such exceptions to the general prohibition should be narrowly tailored to prescribe procedures for these situations, including protocols for preserving these communications. It must be made clear, though, that use of personal email is a narrow exception to the general rule that government employees must use official email accounts for emails involving government business.[171]

4. Institutional Oversight

To effect the change sought by this Note's solution, institutional measures aimed at ensuring compliance should be taken. Noncompliance with transparency laws is well documented, and the need for institutional oversight in this arena is likewise not a novel concept.[172] An example of such an institutional oversight mechanism is the recently created Office of Government Information Services, which is responsible for counseling

---

167. *See id.*

168. *See id.*

169. GINSBERG, *supra* note 24, at 6 n.25.

170. Carroll, *supra* note 130 ("High-level officials . . . need the flexibility to sometimes use a personal email, such as responding to a national security emergency in the middle of the night."). As discussed *infra*, increased spending on government IT would facilitate more secure and convenient access to government email accounts. Thus, the increased availability of official accounts on mobile devices and otherwise should obviate some of the need to use private email when government employees are away from their work computer.

171. The exception could be simply added by leaving 44 U.S.C. §§ 2209(a) and 2911(a) intact (i.e., retain the word "unless") and inserting a subsection (1) stating: "the official electronic messaging account of the covered employee is practically inaccessible. Any such electronic message shall be copied or forwarded to an official electronic messaging account not later than twenty days after the transmission of the original message."

172. *See* Maria H. Benecki, *Developments Under the Freedom of Information Act—1987*, 1988 DUKE L.J. 566, 579–80 (describing Congressional hearings and proposals in 1986 and 1987 regarding the introduction of a FOIA Tribunal or Ombudsman).

agencies on FOIA compliance, suggesting policy changes, and mediating disputes between requesters and agencies.[173] An impartial ombudsman operating outside the ambit of the regulated agencies would give this Note's solution the operational capability to influence email retention.

Assuming a record is preserved, illegitimate concealment of the record is unlikely, because FOIA administrators generally have no political stake in disclosure versus nondisclosure; indeed, their interests may even cut in favor of disclosure.[174] Due to their relative impartiality, FOIA administrators would be more accurate in their categorization of records than the individuals creating or receiving the email records.

B. *Increasing Security*

Allowing government employees to transmit government records on personal email accounts is fraught with risk.[175] Bringing all (or, at least, *more*) government emails under the protection of government servers would yield significant security improvements. Given the sensitivity and importance of information handled by organizations like the Departments of State and Defense, these risks should be minimized to the greatest degree possible. The best way to achieve consistent and comprehensive security of our government's valuable digital information is to restrict transmission of official emails to accounts of official networks.

A consistent "security fence" protecting the lot of government emails is needed to reduce the risks posed by the transmission of official emails on unprotected servers.[176] By neglecting to use a State Department email address during her tenure, Hillary Clinton ostensibly rejected protection by the State Department's IT department and the National Security Agency.[177] Of course, she could have enjoyed similarly sophisticated defenses with an email address hosted by an email provider like Yahoo or Gmail,[178] but even security provided by Internet companies varies between providers and cannot guarantee an account will not be hacked.[179] The most important security benefit of this Note's solution is enhanced consistency of email protection across the spectrum of government emails.

---

173. *See* 5 U.S.C. § 552(h) (2012).

174. Seth F. Kreimer, *The Freedom of Information Act and the Ecology of Transparency*, 10 U. PA. J. CONST. L. 1011, 1047–48 (2008) ("Many of the decisions regarding FOIA requests are made at a line level by career bureaucrats who have no political stake in disclosure or nondisclosure and who can do their jobs most easily by following regulations in good faith.").

175. *See supra* Section III.B.

176. *See* Greenberg, *supra* note 137.

177. *See id.*

178. *See id.*

179. *See* Zetter, *supra* note 142.

C. *Modernizing Information Technology*

While enhancing the consistency of officials' email protections would be a major security improvement, inadequacies of government IT should not be ignored. Government agencies have been criticized of late for their vulnerability to cyber threats and their antiquated IT. Significant investment is needed to meet these challenges.

In recent years, government agencies have repeatedly been the targets of successful hacking attacks.[180] Notably, hackers recently breached the State Department's unclassified email system—one of the very systems this Note suggests would be preferable to a personal email account.[181] Some have even made the case that email accounts hosted by private Internet companies are less prone to hacks than government email accounts.[182]

Inspections of federal agencies' IT systems confirm the anecdotal evidence that these systems are deficient. A recent study examining federal information security found "persistent weaknesses at agencies . . . demonstrat[ing] the need for improved security."[183] A separate audit concluded that State Department information-security protocols did not meet federal requirements.[184]

Beyond questions of email security, some have complained that government IT is outdated and inefficient.[185] One former federal employee likened working for the government to "stepping in a time machine."[186] Moreover, secure mobile phones capable of handling

---

180. *See* David Alexander, *The OPM Hack Was a Lot Worse than Previously Disclosed*, HUFFPOST POL. (Sept. 23, 2015, 3:07 PM), http://www.huffingtonpost.com/entry/opm-hack_5602f64be4b08820d91b59c2; *US Centcom Twitter Account Hacked by Pro-IS Group*, BBC (Jan. 12, 2015), http://www.bbc.com/news/world-us-canada-30785232.

181. *See* Nicky Woolf, *State Department Email Attack 'Fits Pattern' of Russian Hackers, Says Expert*, GUARDIAN (Nov. 17, 2014, 1:42 PM), http://www.theguardian.com/us-news/2014/nov/17/state-department-email-attack-shutdown. From the State Department's perspective, the proverbial silver lining is that it was contained to the Department's *unclassified* email system, and no classified information was stolen. *Id.*

182. *See, e.g.*, Johnson, *supra* note 16.

183. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-15-714, FEDERAL INFORMATION SECURITY: AGENCIES NEED TO CORRECT WEAKNESSES AND FULLY IMPLEMENT SECURITY PROGRAMS 18–23, 54 (2015), http://www.gao.gov/assets/680/672801.pdf.

184. Cory Bennett, *State Dept. Cybersecurity Still Lagging, Audit Finds*, HILL (Nov. 20, 2015, 3:02 PM), http://thehill.com/policy/cybersecurity/260942-state-department-cybersecurity-still-lagging-audit-finds.

185. Klapper et al., *supra* note 135 (quoting a State Department policy chief's complaint that Department technology is "so antiquated that NO ONE uses a State-issued laptop and even high officials routinely end up using their home email accounts to be able to get their work done quickly and effectively").

186. Johnson, *supra* note 16.

classified information are practically inaccessible.[187] Several others have called for the modernization of government IT.[188]

Investment aimed at shoring up flimsy digital defenses could significantly reduce the frequency of successful hacks against the government and could make official email accounts and servers safer than private ones.[189] The cost of operating the classification system is estimated at $14.98 billion.[190] In light of this enormous expense, the federal government should prioritize the modernization of IT that could imperil classified information if neglected further. These improvements would make compliance with transparency laws easier, enabling more complete and secure record preservation.

CONCLUSION

The Hillary Clinton email event sheds light on the extensive shortcomings of current records-retention laws. The conflict of interest inherent in today's self-regulation scheme causes a large proportion of email records to elude preservation. Further, antiquated and inefficient government IT causes many government employees to opt to use private email instead of their official accounts, compounding the issue even further. These emails, which inhabit private email servers, can be practically immune from oversight and thus circumvent transparency laws. Beyond that, security measures protecting private servers are often lacking and can leave sensitive information vulnerable to hacking.

To address the issues associated with government emails on private accounts, the practice of sending such emails should be prohibited. Additionally, government IT should be modernized to securely meet the demands of government employees who are connected to their email

187. Robert O'Harrow Jr., *How Clinton's Email Scandal Took Root*, WASH. POST (Mar. 27, 2016), https://www.washingtonpost.com/investigations/how-clintons-email-scandal-took-root/2016/03/27/ee301168-e162-11e5-846c-10191d1fc4ec_story.html (noting a request by Clinton for a secure mobile device which was "rebuffed" by the NSA). Due to the vast amounts of government communications that are classified, being unable to access these documents from anywhere but a work computer is more than a modest hindrance.

188. Suzanne Nossel, *Don't Blame Hillary for the Classified Email Scandal*, FOREIGN POL'Y (Sept. 30, 2015), http://foreignpolicy.com/2015/09/30/dont-blame-hillary-for-the-classified-email-scandal-state-department-servers/ (noting that the State Department did not offer employees access to cell phones equipped to handle classified emails during Clinton's term as Secretary of State); James Reinl, *CIA Director Hack by Teen Spotlights US Cyber-Frailty*, ALJAZEERA (Oct. 24, 2015, 1:34 PM), http://www.aljazeera.com/indepth/features/2015/10/cia-director-hack-teen-spotlights-cyber-frailty-151024123451489.html.

189. *Id.* ("The US and other cyber-spying governments use their resources looking to exploit cracks in their rivals' systems rather than finding and patching their own vulnerabilities. . . . 'If all the governments and private sectors around the world invested money and cooperated on cyber-security and actually provided this as a public good like we do with national security, we could change the trajectory.'").

190. INFO. SEC. OVERSIGHT OFFICE, *supra* note 98, at 23.

around the clock. These changes will preserve and protect the government's emails. To continue without real change is to perpetuate a faltering system.