University of Richmond Law Review

Volume 51
Issue 3 *National Security in the Information Age: Are We Heading Toward Big Brother? Symposium Issue 2017*

Article 8

3-1-2017

"I Want My File": Surveillance Data, Minimization, and Historical Accountability

Douglas Cox
City University of New York School of Law

"I WANT MY FILE": SURVEILLANCE DATA, MINIMIZATION, AND HISTORICAL ACCOUNTABILITY

Douglas Cox *

INTRODUCTION

Revelations of secret National Security Agency ("NSA") intelligence collection programs and other federal and state surveillance programs have reignited the debate over the relative value of individual privacy rights and national security. This article argues that in this debate greater attention must be paid to the "right to know"—both the individual's "right to know" what records the government collects on them and the public's "right to know" the scope of government surveillance programs—and that federal recordkeeping laws are the appropriate legal mechanism to ensure both long-term government accountability and the historical record.

If government surveillance records are destroyed rather than retained, the ability to hold the government accountable for the collection of that information is greatly diminished. In the debate over publicly disclosed NSA programs, however, "both sides" of the privacy versus security debate appear to agree that the government should *destroy* these records and the debate is limited to how *short* the retention period ought to be. Plaintiffs in cases challenging these collection programs have sought as a primary remedy the immediate destruction, expungement, or purge of records and data.[1] The government, in turn, has defended the legali-

* Attorney and Law Library Professor, City University of New York School of Law. The author previously worked in intelligence while serving in the United States Army. This article underwent prepublication review by the National Security Agency and was cleared for publication. The views expressed are only those of the author.

1. *See, e.g.*, Complaint, Jewel v. Nat'l Sec. Agency, No. 08-4373 (N.D. Cal. Sept. 17, 2008) (seeking order "requiring the destruction of all copies of" plaintiffs' communications seized by the government); Complaint at 10, ACLU v. Clapper, No. 13-3994 (S.D.N.Y. June 11, 2013) (seeking order to NSA "to purge from their possession all of the call records of Plaintiff's communications"); Complaint at 31–32, Klayman v. Obama, No. 13-881 (D.D.C. June 11, 2013) (seeking order that plaintiff's phone and internet records be "expunged

ty of these programs by highlighting compliance with "minimization" procedures that include limited retention periods for certain data as a method for ameliorating privacy concerns.[2] The government has openly promoted its intention to destroy all of the data obtained through its bulk telephony metadata program.[3]

This apparent consensus, that surveillance records should be destroyed in order to protect privacy rights, is in tension with a long history of individuals fighting to *preserve* government records—particularly those that have violated their privacy rights—both in order to access the records and to ensure accountability for surveillance programs. Famously, in 1989, following the fall of the Berlin Wall, East German citizens marched on offices of the Stasi in order to *prevent* the destruction of their files.[4] Their motto was "I want my file!"—an assertion of the "right to know."[5]

The statutory representative of the "right to know" in United States law is the Freedom of Information Act ("FOIA").[6] In the aftermath of public disclosures of sweeping domestic surveillance programs, many individuals have demanded their "files" under both FOIA and analogous state freedom of information laws. In 2013, for example, the NSA reported an 888 percent increase in the number of FOIA and Privacy Act requests from individuals

---

from federal government records.").

2. *See, e.g.*, Official Statement, Office of Dir. of Nat'l Intelligence, Release of 2015 Section 702 Minimization Procedures (Aug. 11, 2016), https://icontherecord.tumblr.com/post/148797010498/release-of-2015-section-702-minimization ("These procedures are intended to protect the privacy and civil liberties of U.S. persons . . . .").

3. *See* Press Release, Office of Dir. of Nat'l Intelligence, ODNI Announces Transition to New Telephone Metadata Program (Nov. 27, 2015), https://www.dni.gov/index.php/newsroom/press-releases/210-press-releases-2015/1292-odni-announces-transition-to-new-telephone-metadata-program ("NSA will destroy the Section 215 bulk telephony metadata as soon as possible upon expiration of its litigation preservation obligations.").

4. *See* Stephen Kinzer, *East Germans Face Their Accusers*, N.Y. TIMES MAG. (Apr. 12, 1992), http://www.nytimes.com/1992/04/12/magazine/east-germans-face-their-accusers.html?pagewanted=all.

5. *Id.* The issue of retention or destruction of records of state security services after the fall of repressive regimes has arisen with some frequency. While some countries have decided to destroy such records to protect privacy, others have preserved them for purposes of accountability and history. *See* ANTONIO GONZÁLEZ QUINTANA, ARCHIVAL POLICIES IN THE PROTECTION OF HUMAN RIGHTS 50–55 (2009), http://www.ica.org/sites/default/files/Report_Gonzalez-Quintana_EN.pdf (discussing historical examples and arguing for preservation).

6. *See* 5 U.S.C. § 552 (2012 & Supp. I 2014); *see also* U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 772–73 (1989) (stating FOIA enforces the rights of citizens to be information about what "their government is up to") (quoting Envtl. Prot. Agency v. Mink, 410 U.S. 73, 105 (1973) (Douglas, J., dissenting)).

wanting to know what records the NSA maintained on them.[7] The NSA's response to these requests was the so-called "Glomar" response, in which the agency asserts that it can neither confirm nor deny whether any such records exist based on national security concerns.[8]

In such cases, an individual's and the public's "right to know" may only fully ripen years, if not decades, in the future when sensitive surveillance records and classified programs are declassified. The NSA's intent to destroy records responsive to such requests, however,—purportedly in order to protect their privacy rights—will thwart these individuals from ever fully satisfying their right to know the extent of government surveillance of their communications and the public may never know the full breadth or scope of these programs, as the historical record may become sanitized.

The subtitle of this symposium—"Are We Heading Toward Big Brother?"—is a particularly apt reference here. In George Orwell's *1984*, the main protagonist Winston Smith was an employee in the Records Department of the Ministry of Truth and part of his responsibilities included destroying historical records in order to shape history to conform with the narrative of the Party.[9]

The dynamic is illustrated with Noam Chomsky's "nonexistent" Central Intelligence Agency ("CIA") file. In response to a researcher's FOIA requests seeking CIA records on Chomsky, the CIA responded not with a "Glomar" response, but with a substantive response stating that "despite thorough and diligent" searches no responsive records were located.[10] The response left the impression that the CIA had *never* maintained records on Chomsky.

---

7. *See* Yamiche Alcindor, *NSA Grapples with Huge Increase in Records Requests*, USA TODAY (Nov. 18, 2013), http://www.usatoday.com/story/news/nation/2013/11/17/nsa-grapples-with-988-increase-in-open-records-requests/3519889/.

8. *See* Marisa Taylor & Jonathan S. Landay, *Americans Find Swift Stonewall on Whether NSA Vacuumed Their Data*, MCCLATCHY (Feb. 11, 2014), http://www.mcclatchydc.com/news/nation-world/national/national-security/article24763393.html. The use of a "Glomar" response was first recognized in a FOIA case involving CIA records related to a submarine ship called the "Glomar Explorer." Phillippi v. Cent. Intelligence Agency, 546 F.2d 1009, 1013 (D.C. Cir. 1976).

9. GEORGE ORWELL, NINETEEN EIGHTY-FOUR 44 (Kindle ed., Planet eBook 2004) (1949) ("And if all others accepted the lie which the Party imposed—if all records told the same tale—then the lie passed into history and became the truth.").

10. John Hudson, *The CIA Has Nothing on Noam Chomsky (No, Really)*, FOREIGN POL'Y (Feb. 27, 2013), http://foreignpolicy.com/2013/02/27/the-cia-has-nothing-on-noam-chomsky-no-really/.

"The CIA Has Nothing on Noam Chomsky (No, Really)," read one headline.[11]

Months later, however, the CIA revised its FOIA response when the FBI found a copy of a CIA record referencing Chomsky and forwarded it to the CIA.[12] As it turned out, a number of historical CIA records provided to, and preserved by, the House Select Committee on Assassinations not only referenced Chomsky, but also indicated that he was a person of interest in Operation CHAOS, a CIA program targeting the activities of anti-war protestors during the Vietnam War.[13]

Ultimately, the reason why the CIA had no records on Chomsky in response to FOIA requests in 2014 was because the CIA destroyed records on United States persons from Operation CHAOS in 1978 with the justification that destroying them was necessary to protect the privacy of those individuals.[14] The effect, though, undermined the public's understanding of the full extent of the program.[15]

To be clear, different government collection programs and different groups of surveillance records and data deserve different treatment. There are meaningful differences between traditional hardcopy records documenting physical surveillance, on one hand, and petabytes of incidentally collected raw data on the other, which may alter the question of whether retention is necessary or desirable to ensure historical accountability. Yet, under current procedures, even records that the National Archives and

11. *Id.*

12. John Hudson, *Exclusive: After Multiple Denials, CIA Admits to Snooping on Noam Chomsky*, FOREIGN POL'Y (Aug. 13, 2013), http://foreignpolicy.com/2013/08/13/exclusive-after-multiple-denials-cia-admits-to-snooping-on-noam-chomsky/.

13. Douglas Cox, *More CIA Records on Noam Chomsky the CIA Could Not Find*, DOCUMENT EXPLOITATION (Oct. 29, 2013), http://www.docexblog.com/2013/10/more-cia-records-on-noam-chomsky-cia.html. The collection of CIA records provided to the House Select Committee on Assassinations is known as the CIA "Segregated Collection" and has been digitized and placed online by the Mary Ferrell Foundation. *See CIA Records Project*, MARY FERRELL FOUND., http://www.maryferrell.org/pages/Featured_CIA_Records_Project.html (last visited Feb. 17, 2017).

14. The destruction of the files was authorized by the Archivist of the United States. CIA, Request for Records Disposition Authority, No. NC1-263-78-1 (Mar. 17, 1978) http://www.dcoxfiles.com/nc1263781.pdf.

15. *See, e.g.*, Agility Pub. Warehousing Co. K.S.C. v. Nat'l Sec. Agency, 113 F. Supp. 3d 313, 334 n.12 (D.D.C. 2015) (noting that even if the government had officially acknowledged the collection program at issue, which might have made collected records subject to FOIA, "the NSA has stated that all records obtained through the program have been destroyed").

Records Administration ("NARA") has assessed as having such historical and legal value that they should be preserved permanently can be summarily destroyed based on orders from the Foreign Intelligence Surveillance Court ("FISC") that fail to consider the value of those records for purposes other than intelligence.[16]

This article argues that limitations on government retention of surveillance data designed to ameliorate privacy concerns must be more meaningfully reconciled with the federal recordkeeping laws, which ensure an objective evaluation of the long-term value of government records and the protection of the "right to know" for individuals and the public. Part I provides relevant background by briefly reviewing the baseline legal regime governing the preservation of federal records[17] and a brief history of repeated attempts to evade these legal requirements in the context of government surveillance records. Part II describes how such evasions argue for applying heightened scrutiny to documentation of modern surveillance programs and how both the FISC and NARA have inadequately addressed the intersection of, and conflict between, retention minimization and the recordkeeping laws. Part III lays out provisional recommendations for balancing the protection of privacy, the "right to know," and historical accountability.

I. FEDERAL RECORDS LAW AND THEIR EVASION

The federal records laws are designed to provide a comprehensive framework for the creation, maintenance, and final "disposition" of federal records, which can include either destruction or preservation in the National Archives.[18] These laws aim to preserve accountability and the historical record by requiring assessments of the legal, historical, and research value of govern-

16. *See infra* notes 73–94 and accompanying text.

17. This article will focus on federal law for the sake of clarity and convenience. Many state records laws and freedom of information laws are based on the federal counterparts, although often with variations that are beyond the scope of this article.

18. The federal records laws are frequently referred to as the "Federal Records Act," although the relevant statutory provisions derive from several different acts, including the Records Disposal Act of 1943, the Federal Records Act of 1950, and the Federal Records Management Amendments of 1976. Records Disposal Act, Pub. L. No. 78-115, 57 Stat. 380 (1943) (codified as amended at 44 U.S.C. §§ 3301–3314 (2012 & Supp. II 2015)); Federal Records Act of 1950, Pub. L. No. 81-754, § 6, 64 Stat. 578; Federal Records Management Amendments of 1976, Pub. L. No. 94-575, 90 Stat. 2723 (codified as amended at 44 U.S.C. §§ 2901-2907 (2012 & Supp. II 2015)).

ment records by both the agencies that create them and the Archivist of the United States (the "Archivist") prior to their destruction.[19] Such requirements serve the statutory goal of preserving "[a]ccurate and complete documentation of the policies and transactions of the Federal Government."[20]

As described below, despite these broad goals, there is a long history of agencies ignoring or actively evading recordkeeping laws especially in the context of government surveillance activities with constitutional implications. The courts have recognized, for example, that "agencies, left to themselves, have a built-in incentive to dispose of records relating to 'mistakes' or, less nefariously, just do not think about preserving 'information necessary to protect the legal and financial rights . . . of persons directly affected by the agency's activities.'"[21]

A. *Federal Records Laws*

Contrary to the popular notion that agencies can avoid records by carrying out business over the phone or in person, the federal records laws expressly obligate agencies to *create* records. In particular, the law requires that agencies "*shall make* and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency."[22] This duty creates a floor that the courts have described as a basic duty "to create and then retain a baseline inventory of 'essential' records."[23] The same provision further defines this duty by requiring that such "adequate and proper documentation" be designed to "furnish the information necessary to protect the legal and financial rights" not only of the government, but also of "persons directly affected by the agency's activities."[24]

19. *See* 44 U.S.C. §§ 3303–3303a (2012 & Supp. II 2015); *see also* Armstrong v. Exec. Office of the President, 1 F.3d 1274, 1285, 1287 (D.C. Cir. 1993) (referencing "Congress' evident concern with preserving a *complete* record of government activity for historical and other uses").

20. 44 U.S.C. § 2902 (2012).

21. Am. Friends Serv. Comm. v. Webster, 720 F.2d 29, 41 (D.C. Cir. 1983) (quoting 44 U.S.C. § 3101 (2012)).

22. 44 U.S.C. § 3101 (2012) (emphasis added).

23. *See Armstrong*, 1 F.3d at 1286.

24. 44 U.S.C. § 3101.

The federal records laws further require that agencies establish "safeguards against the removal or loss of records" and instruct agency employees that agency records may not be "alienated or destroyed" except in compliance with the federal records laws.[25] These laws place an affirmative duty on the agency to "notify the Archivist of any actual, impending, or threatened unlawful removal . . . or other destruction of records."[26]

Regarding the disposal of records, the basic rule is agencies may not destroy any federal records unless and until the Archivist has approved of such destruction.[27] In practice, agencies submit proposed lists or schedules of records identifying categories of agency records. With these proposed schedules, agencies also propose whether each category should be either permanent records—which will eventually be transferred to the National Archives—or temporary records.[28] If the latter, the agency will propose retention periods that can range from instructions to destroy immediately or to retain for a period of time, then destroy.[29] Such temporary records should consist of those that "do not appear to have sufficient value to warrant their further preservation by the Government" when they are no longer "needed by [the agency] in the transaction of its current business."[30]

Agency assessments of the value of federal records are not, however, dispositive. NARA examines these proposed schedules and undertakes an independent assessment of the value of the categories of records.[31] The standard is similarly whether the categories listed as temporary records "do not, or will not after the

25. 44 U.S.C. § 3105 (2012 & Supp. II 2015).

26. *Id.* § 3106 (2012 & Supp. II 2015). Crucially, the requirement to maintain and preserve records applies to *all* records, not just those necessary to satisfy the baseline "adequate and proper documentation" standard. *See, e.g.*, *Armstrong*, 1 F.3d at 1286–87 (holding that the federal records laws "mandate that *all* records" be preserved "whether or not related to 'adequate documentation'" and they can only be destroyed "in accordance with explicit statutory directives"); Rohrbough v. Harris, 549 F.3d 1313, 1319 (10th Cir. 2008).

27. *See* 44 U.S.C. § 3314 (2012) (stating that the statutory procedures "are exclusive, and records of the United States Government may not be alienated or destroyed except under this chapter"); *see also Armstrong*, 1 F.3d at 1278 (stating the federal records laws prescribe "the exclusive mechanism for disposal of federal records").

28. *See* 36 C.F.R. § 1220.18 (2016) (defining permanent record and temporary record).

29. See *Records Control Schedules (RCS)*, NAT'L ARCHIVES, http://www.archives.gov/records-mgmt/rcs/ (last visited Feb. 17, 2017). For examples of records schedules approved by the Archivist, with retention periods such as five, ten, twenty, or thirty years, see 36 C.F.R. § 1220.12 (2016) (describing the records scheduling and appraisal process).

30. 44 U.S.C. § 3303 (2012 & Supp. II 2015).

31. *Id.* § 3303a(a) (2012 & Supp. II 2015).

lapse of the period specified, have sufficient administrative, legal, research, or other value to warrant their continued preservation by the Government."[32] NARA's review of proposed records schedules and record retention periods may include reviewing the covered records, or samples thereof, and sometimes involves lengthy negotiations with the agency if there is disagreement.[33]

If and when there is agreement on an agency records schedule, the Archivist signs it and "empower[s] the agency to dispose of those records" in accordance with the schedule.[34] NARA also proactively promulgates records schedules designed to cover generic types of routine records common to all agencies in schedules called General Records Schedules.[35]

In sum, the federal records laws are designed to involve a neutral arbiter of the value of agency records to try to ensure that they are preserved or destroyed based on whether they are valuable, rather than whether they reflect positively on an agency. As one early National Archives leader noted, "[a]n archivist is not an interested party with respect to the preservation of evidence, whether favorable or unfavorable to an agency's administration. He will not judge of its partiality; he is interested only in preserving all the important evidence."[36]

B. *A Primer on Evading Records Laws*

For as long as there have been federal recordkeeping laws, however, there have been attempts to evade them, especially in the context of traditional government surveillance records. The techniques employed include finding ways to exclude documents from the federal records laws altogether or taking advantage of ambiguities in approved schedules in order destroy records that would otherwise be problematic to an agency. A brief review of several such techniques follows.

---

32. *Id.*

33. *See* Steven Aftergood, *National Archives Tackles Email Management*, FAS.ORG (Apr. 10, 2015), http://fas.org/blogs/secrecy/2015/04/nara-capstone/ (noting "trade offs" must be made to ensure an e-mail management regime).

34. 44 U.S.C. § 3303a(a).

35. *Id.* § 3303a(d) (2012); 36 C.F.R. § 1220.12(d) (2016) (noting that the Archivist "issues General Records Schedules (GRS) authorizing disposition, after specified periods of time, of records common to several or all Federal agencies").

36. T.R. SCHELLENBERG, MODERN ARCHIVES: PRINCIPLES AND TECHNIQUES 29 (1956).

1. "Do Not File" Procedures

For decades, the FBI utilized special "Do Not File" procedures in which certain records were maintained outside of normal agency filing systems in order to limit their accessibility and retention.[37] As described by historian Athan Theoharis:

> Under these procedures, extremely sensitive FBI documents were not serialized and were filed separately, so that they could be destroyed or denied. Under a "Do Not File" procedure, FBI officials could affirm that a search of the central files disclosed no additional documents (particularly pertaining to the Bureau's illegal or "embarrassing" activities).[38]

The FBI's use of "black bag jobs," for example, which involved surreptitiously entering private property without a warrant were handled under such "Do Not File" procedures with the result that "[n]o permanent records were kept for approvals" of such operations and after review, "these records were destroyed."[39]

2. Nonrecords

Another technique is the expansive use of what ought to be a limited, technical carve-out from the federal recordkeeping laws for nonrecords or nonrecord material. The significance of an agency categorizing documents or data as a nonrecord is that it removes such material from the integrated legal framework for federal records and allows the agency to destroy it at its discretion.[40]

Under the federal records laws, "records" are defined quite broadly to include:

---

37. *See* SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK II: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755 (2d Sess. 1976), at 148–49, (describing "Do Not File" procedure as a "special filing system" that allowed documentation of "illegal operations" such as "break-ins" and surveillance to be "systematically destroyed") [hereinafter CHURCH REPORT BOOK II].

38. Athan G. Theoharis, *In-House Cover-up: Researching FBI Files*, *in* BEYOND THE HISS CASE: THE FBI, CONGRESS AND THE COLD WAR 20, 21–22 (Athan G. Theoharis ed., 1982).

39. CHURCH REPORT BOOK II, *supra* note 37, at 61–62.

40. 36 C.F.R. § 1222.16(b)(3) (2016) ("Nonrecord materials should be purged when no longer needed for reference. NARA's approval is not required to destroy such materials.").

> [A]ll recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency . . . as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.[41]

Nonrecords are documentary materials that fail to satisfy even this broad definition. NARA regulations define "nonrecord materials" as "U.S. Government-owned documentary materials that do not meet the conditions of records status."[42] The original concept of nonrecords arose innocently enough. A portion of the legislative history of the Records Disposal Act of 1943, which provided the original definition of records that remains largely intact, indicated that Congress wanted to "make it clear that [agencies] are not obliged to consider every scrap of paper on which writing or printing appears as a record."[43]

The concept of nonrecords, however, expanded over time based on increasingly broad determinations that documents failed to meet even the low hurdle of the definition of record on the basis that they were not "appropriate for preservation."[44] A NARA Task Force in 1988 noted, for example, a "trend" following the passage of FOIA, in which "a number of agencies attempted to exclude certain types of information from disclosure by labeling the materials containing such information as nonrecord" given that FOIA applies to agency records.[45]

The most egregious example of the expansive use of the nonrecord category is the CIA's destruction of videotapes depicting the brutal interrogations of detainees.[46] A CIA spokesperson publicly explained the CIA's position by stating, "[t]he bottom line is that the[ ] tapes were not federal records as defined by the Federal Records Act."[47] NARA recently reopened an inquiry into whether

41. 44 U.S.C. § 3301(a)(1)(A) (2016).

42. 36 C.F.R. § 1222.14 (2015).

43. H.R. REP. NO. 78-559, at 1 (1943), *reprinted in* 1943 U.S.C.C.S. 2-140, 2-141; *see also* NAT'L ARCHIVES & RECORDS ADMIN., NARA AND FEDERAL RECORDS: LAWS AND AUTHORITIES AND THEIR IMPLEMENTATION 6 (1988) [hereinafter NARA TASK FORCE].

44. NARA TASK FORCE, *supra* note 43, at 7.

45. *Id.* at 6.

46. *See generally* Douglas Cox, *Burn After Viewing: The CIA's Destruction of the Abu Zubaydah Tapes and the Law of Federal Records*, 5 J. NAT'L SECURITY L. & POL'Y 131 (2011).

47. Michael Isikoff, *The CIA and the Archives*, NEWSWEEK (Dec. 21, 2007), http://www.

the CIA tape destruction constituted an authorized destruction of federal records, the results of which are not yet public.[48]

3. "Approved" Destruction

Another frequent issue is agency destruction of records pursuant to an Archivist-approved records schedule that is either misunderstood or misapplied (intentionally or inadvertently). In the late 1990s, for example, a *New York Times* article revealed that the CIA had destroyed records related to its involvement in the 1953 coup in Iran.[49] As a result, NARA began an inquiry into the possible unauthorized destruction of records.[50] In response, the CIA claimed that any destruction had been authorized by records schedules approved by the Archivist.[51] NARA concluded, however, "no schedules in effect" when the records were destroyed "provided for the disposal of records relating to covert actions and therefore the destruction of records relating to Iran was unauthorized."[52]

Sometimes the relevant records schedule, or what records they cover, is difficult to discern. In 2010, for example, an employee alleged that the Securities and Exchange Commission ("SEC") had been improperly destroying investigative records, which prompted several investigations.[53] The records at issue documented "matters under inquiry," which are an early part of the SEC investigative process.[54] One problem was discerning whether these records were subject to an Archivist-approved records schedule

---

newsweek.com/cia-and-archives-94445.

48. *See* Douglas Cox, *The CIA and the Unfinished National Archives Inquiry*, JURIST (Oct. 3, 2012), http://www.jurist.org/forum/2012/10/douglas-cox-cia-records.php; Michael Isikoff, *CIA Faces Second Probe Over Videotape Destruction*, NBC NEWS (Nov. 10, 2010), http://www.nbcnews.com/id/40115878/ns/us_news-security/t/cia-faces-second-probe-over-videotape-destruction. The author currently has an outstanding FOIA request for any additional records related to the NARA inquiry.

49. Tim Weiner, *C.I.A. Destroyed Files on 1953 Iran Coup*, N.Y. TIMES (May 29, 1997), http://www.nytimes.com/1997/05/29/us/cia-destroyed-files-on-1953-iran-coup.html.

50. NAT'L ARCHIVES & RECORDS ADMIN., RECORDS MANAGEMENT IN THE CENTRAL INTELLIGENCE AGENCY 29 n.1 (2000).

51. *See id.*

52. *Id.*

53. *See* David S. Hilzenrath, *A Different Story Emerges on SEC Record Purges*, WASH. POST (Sept. 5, 2011), https://www.washingtonpost.com/business/economy/a-different-story-emerges-on-sec-record-purges/2011/09/02/gIQALBh44J_story.html?utm_term=.6f654f0b5b3f.

54. *Id.*

that required a twenty-five-year retention period for "preliminary investigations" or whether they were not covered by any records schedule.[55] The SEC Office of Inspector General ultimately found that the SEC destroyed documents that should have been preserved as federal records.[56]

Finally, there have been situations in which records schedules approved by the Archivist are found by a court to be inadequate and not in compliance with federal records laws. The D.C. Circuit, for example, held that an Archivist-approved FBI schedule, which allowed the FBI to screen investigative files, selecting some for retention and others for destruction based on certain criteria, failed to comply with the law.[57] In particular, the court held that the schedule did not adequately comply with the obligation to preserve information "pertaining to the legal rights of persons directly affected by the FBI's activities."[58]

II. SECRET SURVEILLANCE DATA AND RECORDKEEPING

This history of government attempts at evading recordkeeping laws for traditional surveillance activities can lead to reasonable questions about whether any presumption of good faith is appropriate when the government justifies the destruction of modern surveillance data on privacy grounds, or whether such justifications could be pretextual. At the very least, it is reasonable to approach retention policies related to such data with caution. This includes the status of surveillance data under the federal records laws as well as minimization procedures limiting retention of collected data that are designed to minimize privacy intrusions, but which can also risk minimizing the right to know and historical accountability.

---

55. *Id.*

56. SEC. EXCHANGE COMM., OFFICE OF INSPECTOR GEN., REPORT OF INVESTIGATION, CASE NO. OIG-567, DESTRUCTION OF RECORDS RELATED TO MATTERS UNDER INQUIRY AND INCOMPLETE STATEMENTS TO THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION REGARDING THAT DESTRUCTION BY THE DIVISION OF ENFORCEMENT 2 (2011).

57. Am. Friends Serv. Comm. v. Webster, 720 F.2d 29, 68–69 (D.C. Cir. 1983).

58. *Id.* at 36. The district court had gone even further, finding that "it is clear that the FOIA influenced the drafting" of the schedule and "reflected a bias, on impermissible grounds, in favor of the destruction rather than the preservation of government records." Am. Friends Serv. Comm. v. Webster, 485 F. Supp. 222, 233 (D.D.C. 1980).

A. *Data as Nonrecords and Records Schedules*

One issue is the extent to which agencies are treating increasingly sophisticated forms of surveillance data as records subject to the federal records laws or as nonrecords. In 2015, as one example, documents released via FOIA revealed that the Internal Revenue Service ("IRS") had been using a Stingray system, a "cell-site simulator" that mimics cell phone towers, in order to help determine the location of specific mobile phones.[59] In a July 2016 Privacy Impact Assessment, the IRS addressed its use of Stingrays and provided a rare glimpse into the retention of such data.[60] In response to the question of whether Stingray data was covered under an "archivist approved" records schedule "for the retention and destruction of official agency records stored in this system," the IRS indicated it was not.[61] "Data from the Stingray is purged after completion of the operation," the IRS stated, on the basis that "[i]t is not the official repository for data and documents and does not require National Archives approval to affect data disposition."[62] The IRS further noted, without explanation, that "[a]ny new *records* generated by the system" would be made subject to the IRS records management program.[63] Therefore, where the line is being drawn between nonrecords and records for such data remains opaque.

Similarly, even when certain forms of data are treated as records subject to the records laws, agencies can fail to provide clarity about which records schedules or which retention periods apply. In 2014, for example, the Law Library of Congress conducted a global survey of laws regarding the collection of biometric data of passport applicants and passport holders.[64] The study covered types of biometric databases, the purposes of those databases, access restrictions related to them, and the duration of data reten-

59. Nicky Woolf & William Green, *IRS Possessed Stingray Cellphone Surveillance Gear, Documents Reveal*, THE GUARDIAN (Oct. 26, 2015), https://www.theguardian.com/world/2015/oct/26/stingray-surveillance-technology-irs-cellphone-tower.

60. *See* INTERNAL REVENUE SERV., PRIVACY IMPACT STATEMENT NO. 1832 (2016), https://www.irs.gov/pub/irs-utl/ci-use-stingray2-pia.pdf.

61. *Id.*

62. *Id.*

63. *Id.* (emphasis added).

64. LAW LIBRARY OF CONGRESS, BIOMETRIC DATA RETENTION FOR PASSPORT APPLICANTS AND HOLDERS 1 (2014), https://www.loc.gov/law/help/biometric-data-retention/biometric-passport-data-retention.pdf.

tion.[65] While the Law Library of Congress was able to locate definitive retention periods for a number of other countries, it was unable to verify how long the United States Department of State retains such biometric records.[66] In a lengthy footnote, the authors explained that the records schedule cited by the Department of State included a wide variety of different categories of records whose retention periods varied from permanent to six months "to be destroyed 'when active agency use ceases'" and it was unclear which applied.[67] Thus, as far as the public knows, the State Department may be retaining biometric data for somewhere between six months and forever.

B. *FISC, Minimization, and Federal Records*

A more wide-ranging example is the interaction—or disconnect—between Foreign Intelligence Surveillance Act ("FISA") minimization procedures and the federal records laws. As explained in more detail below, the recordkeeping laws essentially fall through the cracks; the Foreign Intelligence Surveillance Court ("FISC") basically ignores these laws in approving minimization procedures, while NARA—tasked with enforcing the records laws—largely defers to the minimization procedures the FISC imposes.

1. FISA Retention Minimization

Minimization procedures, which are a feature of both Title III wiretaps and FISA, are generally designed to minimize the overcollection, use, and—in the FISA context—retention of surveillance data.[68] Controversies over minimization procedures have largely centered on whether they are effective at protecting privacy or whether excessive exceptions and loopholes undermine their usefulness and purpose.[69]

---

65. *Id.*

66. *Id.* at 8 ("No clear statement is provided regarding the duration of the storage of data. . . .").

67. *Id.* at 13 n.83.

68. *See generally* 18 U.S.C. § 2518 (2012) (establishing standards for Title III wiretaps to "minimize the interception of communications not otherwise subject to interception under this chapter"); 50 U.S.C. § 1801(h) (2012) (defining "minimization procedures" under FISA).

69. *See, e.g.*, Jake Laperruque, *Updates to Section 702 Minimization Rules Still Leave*

FISA defines minimization procedures, in relevant part, as:

> specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and *retention*, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.[70]

FISA minimization procedures publicly released by the Director of National Intelligence provide examples of *retention* minimization. Under such procedures, for example, certain FISA-acquired data "will be destroyed upon recognition," while other data "may not be retained longer than" two years or five years or some other period.[71] Retention periods for data under certain FISA programs, moreover, remain classified. Under FBI minimization procedures for section 702 collection, for example, certain FISA-acquired information "shall be destroyed [redacted] from the expiration date of the certification authorizing the collection."[72]

The incomplete reconciliation between FISA minimization and other preservation obligations was highlighted in a remarkable series of FISC opinions dealing with the relevance of FISA-acquired data in other litigation. In 2014, the government filed an ex parte motion seeking an amendment to the minimization procedures for section 215 metadata collection based on other pending, non-FISC civil lawsuits.[73] The then-existing minimization

---

Loopholes, CTR. FOR DEMOCRACY & TECH. (Feb. 9, 2015), https://cdt.org/blog/updates-to-section-702-minimization-rules-still-leave-loopholes/. Regarding Title III minimization procedures, see Seth M. Hyatt, *Text Offenders: Privacy, Text Messages, and the Failure of the Title III Minimization Requirements*, 64 VAND. L. REV. 1347, 1351 (2011) ("Courts have spent more than twenty years watering [minimization requirements] down, leaving behind a bizarre, hollowed-out protection that serves as a procedural nuisance to law enforcement without providing meaningful protection to individual privacy.").

70. 50 U.S.C. § 1801(h)(1) (2012) (emphasis added).

71. *See, e.g.*, NAT'L SEC. AGENCY, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 7 [hereinafter NSA SECTION 702 MINIMIZATION PROCEDURES], https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf.

72. *See, e.g.*, FED. BUREAU OF INVESTIGATION, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 23, https://www.dni.gov/files/documents/2015FBIMinimization_Procedures.pdf.

73. *In re* Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, at 1–2, No. BR 14-01 (FISA Ct., Mar. 7, 2014), http://www.fisc.uscourts.gov/sites/default/files/BR%2014-01%20Opinion-1.pdf.

procedures required that collected telephone metadata would be "destroyed no later than five years (60 months) after its initial collection."[74] The government's motion sought authorization for retention longer than five years—subject to additional access and use restrictions—"while six civil matters currently pending in various courts are litigated."[75]

The FISC initially denied the proposed amendment to the minimization procedures on the grounds that, as the government led the court to believe, the only conflicting preservation obligation at issue was the "general obligation of civil litigants to preserve records that could potentially serve as evidence."[76] The FISC reasoned that because minimization procedures were required by statute they "displaced" the "general obligation to preserve records that may be relevant to civil matters," because the latter is only "a matter of federal common law."[77] The FISC later reversed this decision, however, and allowed longer retention, subject to additional restrictions, after plaintiffs in the non-FISC cases obtained restraining orders against the government's data destruction.[78]

Those plaintiffs also formally advised the FISC of other cases and earlier preservation orders the government had failed to disclose in its initial ex parte motion to the FISC.[79] The FISC then issued an order questioning the government's compliance with the duty of candor, stating that the government "should have made the FISC aware of the preservation orders."[80] The FISC added that "[n]ot only did the government fail to do so" but that documents filed by the plaintiffs suggested that "the government sought to dissuade plaintiffs' counsel from immediately raising this issue with the FISC."[81] The FISC ordered the government to explain "why it failed to notify [the FISC] of the preservation orders."[82] In response, the government filed a *mea culpa* stating that "[w]ith the benefit of hindsight, the Government recognizes"

74. *Id.* at 2 (quoting minimization procedures).

75. *Id.* at 5.

76. *Id.* at 2.

77. *Id.* at 3–4.

78. *In re* Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 14-01, at 3–5 (FISA Ct., Mar. 12, 2014).

79. *In re* Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 14-01, at 4–6 (FISA Ct., Mar. 21, 2014).

80. *Id.* at 8–9.

81. *Id.* at 9.

82. *Id.* at 9–10.

that "it should have made [the FISC] aware of those preservation orders" and "regrets its omission."[83]

The FISC's attempt at balancing preservation obligations conflicting with FISA minimization procedures was remarkable for several reasons. First, the FISC essentially treated the request as an issue of first impression, which seems to confirm that the FISC had not previously considered how to reconcile retention minimization with conflicting preservation duties in earlier opinions, many of which remain classified.[84] In the end, the court's analysis simply fell back on a generic canon that federal common law "may be displaced by statute whenever Congress speaks directly to the issue."[85]

Second, the FISC very narrowly interpreted the duty to preserve relevant evidence by confining its analysis only to the specific pending cases of which it was made aware by the government.[86] The duty to preserve relevant evidence, however, extends not only to pending cases, but also to reasonably foreseeable litigation.[87] Indeed, the first case the FISC cited for the duty to preserve relevant evidence was *Kronisch v. United States*.[88] In *Kronisch,* the Second Circuit held that the CIA could be subject to spoliation sanctions for destroying evidence of its MKULTRA program, in which the CIA administered LSD to individuals without their knowledge.[89] This holding was despite the fact that the events at issue in *Kronisch* occurred in 1952, the destruction

83. Response of the United States of America to the Court's March 21, 2014 Opinion and Order at 2, *In re* Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 14-01 (FISA Ct., Apr. 2, 2014).

84. *See In re* Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 14.01, at 3, 8 n.7 (FISA Ct., Mar. 7, 2014) (stating that the "Court has not found any case law supporting the government's broad assertion" and that "cited legislative history sheds no light on what is before the Court").

85. *Id.* at 4 (citing Am. Elec. Power Co. v. Conn., 564 U.S. 410, 423 (2011)).

86. *See In re* Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 14.01, at 6 (FISA Ct., Mar. 12, 2014) (requiring retention "[p]ending resolution of the preservation issues" in specific cases).

87. *See, e.g.*, West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999) (defining spoliation as the destruction of evidence "in pending or reasonably foreseeable litigation"). *See generally* MARGARET M. KOESEL & TRACEY L. TURNBULL, SPOLIATION OF EVIDENCE: SANCTIONS AND REMEDIES FOR DESTRUCTION OF EVIDENCE IN CIVIL LITIGATION (Am. Bar Ass'n 3d ed. 2013) (discussing federal and state law spoliation issues).

88. *In re* Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 14.01, at 2–3 (FISA Ct., Mar. 7, 2014).

89. Kronisch v. United States, 150 F.3d 112, 126, 132 (2d Cir. 1998).

of the documents occurred in 1973, and the case was not brought until ten years later in 1983.[90]

Third, the FISC made no mention of the federal records laws, which provide a potentially conflicting *statutory* basis for preserving records based on a far more comprehensive assessment of their legal, administrative, and historical value.[91] Indeed, litigation preservation obligations themselves—dismissed by the FISC as mere "common law"—are incorporated by statute, regulation, and records schedules into the federal records laws. Federal criminal law makes willfully and unlawfully destroying federal records a felony,[92] the federal records laws require agencies to undertake administrative efforts to prevent such unlawful destruction,[93] and NARA regulations define such unlawful destruction to include the "disposal of a record subject to" a "litigation hold, or any other hold requirement to retain the records."[94]

Following this series of FISC opinions, subsequent FISA minimization procedures contain an exception from destruction for situations in which "the Department of Justice advises NSA in writing that such information is subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation."[95] Indeed, in the context of FISA Section 215 data, the sole reason the government has not yet destroyed all of the telephone metadata collected under the program is due to a carve-out for such ongoing litigation.[96]

---

90. The CIA's justification for the destruction of the documents was claimed to be, in part, to "preserve the confidential identities of outside participants in the MKULTRA program" and to "prevent incomplete documents from being misunderstood." *Id.* at 127.

91. *See supra* Part I.A.

92. *See* 18 U.S.C. § 2071(a) (2012) ("Whoever willfully and unlawfully . . . destroys . . . any record . . . shall be fined under this title or imprisoned not more than three years, or both.").

93. *See* 44 U.S.C. §§ 3105–06 (2012 & Supp. II 2015) (requiring agency heads to establish safeguards against the loss of records, advise employees of penalties for the "unlawful removal or destruction of records," and "notify the Archivist of any actual, impending, or threatened unlawful removal, defacing, alteration or destruction of records").

94. 36 C.F.R. § 1230.3(b) (2015). As another example, the CIA has an Archivist-approved schedule that requires the preservation of "[r]ecords relating to actual or impending litigation." *See* CIA, Request for Records Disposition Authority, No. NC1-263-85-1, (Mar. 26, 1985), http://www.dcoxfiles.com/851.pdf.

95. *See, e.g.*, NSA SECTION 702 MINIMIZATION PROCEDURES, *supra* note 71, at 8.

96. Office of the Dir. of National Intel, *Minimization Procedures Applicable to the Retention of Bulk Metadata Produced as Part of the Section 215 Program*, IC ON THE RECORD, (Jul. 25, 2016), https://icontherecord.tumblr.com/post/147962934793/minimization-procedures-applicable-to ("Although the government is no longer accessing bulk metadata produced by telecommunications providers under the Section 215 program for analytic pur-

The question becomes whether and why the FISC and the minimization procedures should limit such an exception to the specific scenario of litigation holds, rather than extending it to incorporate records responsive to FOIA requests or broader retention categories under the federal records laws.

2. NARA and Retention Minimization

While the FISC has not addressed or acknowledged the possible impact of federal recordkeeping laws in approving minimization procedures, NARA has simultaneously deferred to such court-imposed minimization procedures in a couple of different ways.

First, NARA regulations do contemplate the destruction of records by court order, which could encompass FISC-ordered retention minimization.[97] Those regulations, however, also incorporate additional requirements and safeguards depending upon whether the records to be destroyed by court order have been appraised by NARA archivists as either temporary or permanent records, or whether their value has not been assessed at all (the latter records are categorized as "unscheduled"[98]). "When required by court order (i.e., order for expungement or destruction)," these NARA regulations provide, "an agency may destroy *temporary* records before their NARA-authorized" destruction date.[99] In cases of court orders providing for the destruction of permanent or "unscheduled" records, NARA regulations provide that the "agency must notify" NARA and "[i]f the records have significant historical value, NARA will promptly advise the agency of any concerns over their destruction."[100]

Second, there are several NARA-approved records schedules that expressly contemplate the possible premature destruction of records pursuant to FISA minimization procedures. These approved schedules, however, do not disclose any exploration of the

---

pose, continued retention of this data is necessary to comply with preservation obligations in civil litigation challenging the program, including court orders entered in two of those cases.").

97. 36 C.F.R. § 1226.14(e) (2015).

98. *See id.* § 1220.18 (2015) (defining "unscheduled records" as "[f]ederal records whose final disposition has not been approved by NARA" and noting that "[s]uch records must be treated as permanent until a final disposition is approved").

99. *Id.* § 1226.14(e) (emphasis added).

100. *Id.*

question of whether the retention limitations in such minimization procedures *ought* to properly override the federal records laws.

One publicly available records schedule, for example, covers NSA signals intelligence ("SIGINT") records and data.[101] The schedule contains several categories of SIGINT records whose historical value NARA assessed in different ways.[102] Raw intercepted communications, for example, are temporary records that NSA need only retain "so long as data may be of intelligence interest," while "serialized" SIGINT intelligence reports are treated as permanent records.[103] Within the records schedule, however, an exception is added for several record categories that states: "[a]ny data that contains, or could contain, U.S. person information has legal ramifications. There are strict timelines for retention of this data, and it must be handled in accordance with . . . any special minimization procedures that govern the retention of that data."[104] As an example, it states that "[f]or data collected pursuant to . . . (FISA) or Protect America Act (PAA), retention may only be done in accordance with the minimization procedures for that data."[105]

Crucially, this "exception" for destruction pursuant to minimization procedures applies even to categories of NSA SIGINT records that NARA archivists assessed as having such historical value that they should be permanent federal records that could otherwise never be destroyed.[106] The significance of this assessment is hard to overestimate. Despite a commonly held belief that NARA maintains a significant portion of government records for historical research, in fact less than 3 percent of federal records are treated as permanent records that are preserved forever.[107]

---

101. Nat'l Sec. Agency, Request for Records Disposition Authority, No. N1-457-08-1 (Jan. 1, 2009), https://www.archives.gov/records-mgmt/rcs/schedules/departments/department-of-defense/defense-agencies/rg-0457/n1-457-08-001_sf115.pdf [hereinafter NSA SIGINT Records Schedule].

102. *Id.* at 1–5.

103. *Id.* at 1.

104. *Id.*

105. *Id.*

106. *Id.* at 2, 4.

107. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-742, FEDERAL RECORDS: NATIONAL ARCHIVES AND SELECTED AGENCIES NEED TO STRENGTHEN E-MAIL MANAGEMENT 6 (2008) ("Of the total number of federal records, less than 3 percent are designated permanent.").

One of these "permanent" NSA record categories is SIGINT "Policy and Program Records."[108] In its appraisal report, NARA archivists determined that these records should be permanently preserved because they contain "unique and important documentation on the formulation and development of SIGINT policy," and this group of records "[r]etains significance for documenting legal rights despite the passage of time" and, among other things, they "document the development and implementation of policies resulting from decisions of the Foreign Intelligence Surveillance Court."[109] In addition, NARA also highlighted that "SIGINT policy [is] highly controversial at this time, and is likely to remain so."[110] Despite this, neither the schedule, nor NARA's appraisal report, indicates any hesitation at concluding that such records can nevertheless be summarily destroyed pursuant to minimization procedures as the schedule allows.

A publicly available FBI records schedule similarly incorporates FISA minimization procedures covering the disposition of electronic surveillance data, including "audio, video and other electronic technologies."[111] The schedule provides for a general eleven-year retention period for covered records, with an added requirement that prior to any such destruction, the FBI "will evaluate the electronic surveillance material related to each case to determine whether or not the records have historical value. If so, the records will be proposed for permanent retention under a separate disposition authority."[112] Yet, despite these assessments the records schedule contains an overriding note that "[a]ll information obtained by the FBI pursuant to the orders of a Foreign Intelligence Surveillance Court (FISC) is subject to the Standard Minimization Procedures approved by the FISC" and "FISA information may be destroyed at any time if the FBI" makes certain determinations.[113]

---

108. NSA SIGINT Records Schedule, *supra* note 101, at 4.

109. Memorandum from Margaret Hawkins, NARA, Agency: National Security Agency, Subject: N1-457-08-1, Oct. 20, 2008. The author obtained the NARA appraisal via FOIA and is available at http://www.dcoxfiles.com/n1457081d.pdf.

110. *Id.*

111. FBI, Request for Records Disposition Authority, No. N1-065-03-2, at 1 (July 12, 2004).

112. *Id.* at 2–3.

113. *Id.* at 2. In particular, the note states that pursuant to the FISC-approved minimization procedures,

> FISA information may be destroyed at any time if the FBI determines that:

Yet another publicly available FBI records schedule encompasses FISA data and records that should *not* have been acquired.[114] Specifically, it covers: "FISA-acquired information collected under an order" that "does not meet the terms of the order (for instance, the collection begins or ends after the time frame of the order or a typographical error has directed the surveillance to the wrong individual or facility), that was collected in error, or suffers from any other legal defect."[115] The approved "[d]isposition" for such records is "TEMPORARY" and the instruction is to "DELETE/DESTROY" within "60 days of informing the FISC of the existence of the materials."[116]

For NARA, the question becomes whether, given its unique responsibilities and statutory authorities, it has done enough to ensure that the letter and spirit of the federal records laws are being followed to the greatest extent possible. Given public concerns over surveillance programs, for which there is limited transparency, NARA is in a unique position to help ensure sufficient records are maintained for long-term accountability.

III. PREVENTING ACCOUNTABILITY MINIMIZATION

A. Handschu *Precedent: "In Accordance With Law"*

Just as historical attempts to evade recordkeeping laws provide useful context in assessing current policies on retention of surveillance data, a seminal federal case on government surveillance of political activity—*Handschu v. Special Services Division*[117]—provides a striking illustration of the question of whether indi-

> a) the information is not pertinent to an authorized responsibility, duty, or function of the FBI . . . or the United States intelligence community and is unlikely to become so;
> b) the information is not of foreign intelligence value . . . ;
> c) the information does not contain evidence of a criminal offense . . . ;
> d) the information does not contain material that is potentially exculpatory of a criminal defendant;
> e) the information does not include privileged communications; and
> f) the information is not subject to any rules or requirements under a FISC order which would preclude its immediate destruction.

Id.

114. FBI, Request for Records Disposition Authority, No. N1-065-09-9, at 2 (Jun. 25, 2009).

115. *Id.*

116. *Id.*

117. Handschu v. Special Servs. Div., 273 F. Supp. 2d 327, 327 (S.D.N.Y. 2003).

vidual rights are protected best by preservation or destruction of surveillance records and provides an example of a reasonable, elegant solution.

Handschu is a federal class action originally filed in 1971 challenging the surveillance activities of the New York Police Department ("NYPD"); it continues to this day.[118] In 1985, after years of litigation and negotiation, the parties proposed a settlement to the court, which ultimately became known as the "Handschu Guidelines."[119] The court's review of the settlement dealt, in part, with the question of what should become of the NYPD records themselves, which documented surveillance of political groups, including the Black Panthers and the Young Lords.[120]

On the issue of whether to preserve or destroy the records, Judge Haight noted, "an almost paradoxical reversal in the parties' positions has taken place during the course of the litigation."[121] "The complaint, filed in 1971," Judge Haight continued, "specifically sought the destruction of the NYPD's political files," but the "[d]efendants resisted that prayer. The police wished to keep its files."[122] In 1974, however, New York State enacted its Freedom of Information Law ("FOIL"), the state equivalent of the federal FOIA.[123] The court noted,

> The passage of the state statute, occurring during the post-Watergate atmosphere of increased inquiries into governmental misconduct, brought about 180-degree changes of course on the part of the present litigants. The plaintiffs, now regarding the police files "as a precious historical and political resource," . . . stopped demanding that the police files be destroyed, and insisted instead that they be preserved and revealed. Defendants now wish to destroy the files.[124]

---

118. *Id.* at 329. As Judge Haight noted in 2007, "There will be a Handschu class action and a judge of this Court in charge of it for as long as New York City stands." Handschu v. Special Servs. Div., 475 F. Supp. 2d 331, 332 (S.D.N.Y. 2007).

119. Handschu v. Special Servs. Div., 605 F. Supp. 1384, 1389 (S.D.N.Y. 1985).

120. *Id.* at 1384–85.

121. *Id.* at 1411–12.

122. *Id.* at 1412.

123. The New York Freedom of Information Law is codified at N.Y. PUB. OFF. L. §§ 84–90 (2016).

124. *Handschu*, 605 F. Supp. at 1412 (citation omitted). The court was quoting Paul G. Chevigny, *Politics and Law in the Control of Local Surveillance*, 69 CORNELL L. REV. 735, 748 (1984). Chevigny's article noted that the *Handschu* case was not unique in this regard, stating, "preservation of the files against the wishes of the police who claim that they would prefer to destroy them has become a major issue in many cases, often more important than any other relief." *Id.*

The court noted that during negotiations the NYPD "sought blanket authority to destroy the files outright," while the plaintiffs "pointedly declined to negotiate a settlement which would authorize destruction of records in derogation of the rights of the public under existing disclosure and preservation statutes."[125]

The settlement language the court finally blessed avoided any *ad hoc*, court-ordered solution, but simply provided for the "disposition" of the files "in accordance with law."[126] Judge Haight identified the relevant laws, including the New York FOIL and the relevant records law established under the New York City Charter, which, like the federal records laws, required that a neutral department of records assess the value of records in determining how long they should be preserved.[127] "The upshot of the settlement," the court concluded,

> is that no intelligence or political files, pre-1955 or post-1955, can be destroyed without the express approval of the City's commissioner of records . . . who is specifically charged by the Charter to base his determination "on the potential administrative, fiscal, legal, research or historical value of the record." . . . I will not assume that the police commissioner would disregard the law by disposing of police records without seeking the requisite approval; nor will I assume that the commissioner of records . . . would not take [his] responsibilities seriously when confronted with such a request.[128]

B. *Recommendations on Balancing Interests*

What follows are some provisional thoughts on ways in which the competing interests of privacy, security, the "right to know," and historical accountability can be meaningfully reconciled in relation to more advanced forms of surveillance data in accordance with law.

---

125. *Handschu*, 605 F. Supp. at 1412 (quoting plaintiff's brief).

126. *Id.* at 1392–93.

127. *Id.* at 1412–13.

128. *Id.* at 1413–14. As a brief coda on the story of these records, in 2014, a historian from Baruch College writing a book on the Young Lords submitted a FOIL request for these records. The response from the NYPD, however, was that they were unable to find them. *See* Nick Pinto, *The NYPD's Records of Its Own Misbehavior Have Mysteriously Vanished*, VILLAGE VOICE (May 20, 2016, 12:29 PM), http://www.villagevoice.com/news/the-nypds-records-of-its-own-misbehavior-have-mysteriously-vanished-8639201. During litgation over the lost files in 2016, however, the city located the files in a Queens warehouse. *See* Joseph Goldstein, *Old New York Police Surveillance Is Found, Forcing Big Brother Out of Hiding*, N.Y. TIMES (June 16, 2016), http://www.nytimes.com/2016/06/17/nyregion/old-new-york-police-surveillance-is-found-forcing-big-brother-out-of-hiding.html.

As an initial measure, surveillance data in all forms should be treated as records subject to the federal records laws.[129] The potential evasion of these laws by categorizing documents or data as nonrecords should be avoided at all costs.[130] To be clear, this would not necessarily require that any data be retained any longer than it is currently. Instead, it would simply ensure that all such data is subject to records schedules to decrease the risk that data of significant value are destroyed without notice to, and authorization from, NARA and the Archivist.

NARA and agencies should also document retention periods for such data in clearly defined records schedules, perhaps organized by surveillance programs, to ensure that approvals of destruction are unambiguous to NARA, the agency, and, where possible, the public. Currently it is unclear, for example, whether controversial NSA programs are covered by public schedules, such as the NSA records schedule governing SIGINT data,[131] or none at all. Requiring more clearly defined schedules would ensure greater transparency about the breadth and type of data agencies are preserving or destroying.[132]

More broadly, NARA, the Attorney General, and FISC should work to meaningfully reconcile the federal records laws with procedures designed to limit retention to protect privacy. In particular, NARA should revisit its apparent conclusion—based on publicly available records schedules described above[133]—that the federal records laws ought to yield to FISC minimization procedures. The Attorney General, who is responsible for adopting minimization procedures, and the FISC, who is responsible for

129. *See* 44 U.S.C. § 3301 (2012 & Supp. II 2015) (defining records).

130. *See supra* notes 40–45 and accompanying text. More broadly, this author and others have argued for abolishing the "nonrecord" category altogether. *See* Cox, *supra* note 46, at 174 ("Congress could control misuse of the 'nonrecord' category, for example, by expanding the statutory definition of 'record' to encompass more, if not all, agency documents."); *see also* GARY M. PETERSON & TRUDY HUSKAMP PETERSON, ARCHIVES & MANUSCRIPTS: LAW 15 (1985) ("Perhaps the best approach is to define all agency documents as records" and authorize destruction of marginal documents through records schedules).

131. *See* NSA SIGINT Records Schedule, *supra* note 101.

132. It could also ensure that NARA's appraisal of the value of such data for assessing proper retention periods—which would vary from program to program—is fully informed and accurate.

133. *See supra* notes 101–16 and accompanying text.

approving them,[134] should take the federal records laws into consideration in their analysis.

To be clear, NARA and FISC could ultimately conclude that FISC retention minimization *ought* to overrule any inconsistency with the federal records laws. Support for such a conclusion could come from passages in FISA that provide for surveillance orders "notwithstanding any other law."[135] Or on a more general theory that it is "assume[d] that Congress is aware of existing law when it passes legislation" and therefore Congress was impliedly superseding any conflicting, preexisting recordkeeping laws when it established retention minimization in FISA in 1978.[136] If this is the position of FISC or NARA, then, they ought to address it transparently. Their failure to do so is inconsistent with guidance that courts "should be mindful of the statutory scheme governing disposal of government records."[137] In particular, the Third Circuit has noted that in issuing confidentiality or protective orders "[c]ourts must exercise caution" so as "not to demand" that an agency "destroy government documents . . . in conflict with [an agency's] duty to obey the requirements" of the federal records laws.[138]

Any argument that FISA was intended to supersede the federal records laws is suspect. Generally, a court must read potentially conflicting "statutes to give effect to each if [the court] can do so while preserving their sense and purpose."[139] FISA and the federal records laws are not "irreconcilably conflicting" and both provide flexibility.[140] FISA's legislative history, for example, acknowledges

134. *See* 50 U.S.C. § 1801(h) (2012) (defining minimization procedures as "specific procedures, which shall be adopted by the Attorney General"); *id.* § 1806(f) (2012) (establishing a court review procedure "notwithstanding any other law"); Jewel v. Nat'l Sec. Agency, 965 F. Supp. 2d 1090, 1104–05 (N.D. Cal. 2013) (citing the "notwithstanding any other law" language in finding that "FISA preempts the common law doctrine of the state secrets privilege").

135. *See, e.g.*, 50 U.S.C. § 1802(a)(1) ("Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance.").

136. Miles v. Apex Marine Corp., 498 U.S. 19, 32 (1990).

137. Equal Emp't Opportunity Comm'n v. Kronos, Inc., 620 F.3d 287, 303 (3d Cir. 2010).

138. *Id.* at 304; *see also* Sec. Exch. Comm'n v. Jupiter Grp. Capital Advisors, LLC, No. 11-00291, 2012 WL 668830, at *5–6 (D. Haw., Feb. 29, 2012) (remanding issue of protective order containing a document destruction requirement back to magistrate judge to consider restrictions of the federal records laws).

139. Watt v. Alaska, 451 U.S. 259, 267 (1981); *see also* LARRY M. EIG, CONG. RESEARCH SERV., RL 97589 STATUTORY INTERPRETATION: GENERAL PRINCIPLES AND RECENT TRENDS 29 (2011) (discussing standards for repeals by implication).

140. *Watt*, 451 U.S. at 266; EIG, *supra* note 139, at 29.

that it will not always be feasible for "retention" minimization to be accomplished through actual destruction.[141] Retention is just one in a suite of minimization tools. As David Kris and J. Douglas Wilson note:

> The legislative history further explains that there are "a number of means and techniques which the minimization procedures may require to achieve the purpose set out in the definition," including "but not limited to" the "destruction of unnecessary information acquired," or the use of "provisions with respect to what may be filed and on what basis, what may be retrieved and on what basis, and what may be disseminated, to whom and on what basis."[142]

Indeed, examples of this are the amendments to minimization procedures to allow for lengthy retention periods consistent with litigation preservation obligations. When subject to enhanced restrictions on use and access, they provide concrete illustrations of the flexible use of different minimization tools to achieve the larger goal.[143] Further, the amended minimization procedures also suggest that the Attorney General and the FISC have *not* concluded that FISA simply supersedes any potentially conflicting legal obligations.

Also important to the "right to know," the Attorney General and NARA should also consider the proper impact of the thousands of FOIA requests the NSA has received in the aftermath of public disclosures related to NSA surveillance programs. Preservation obligations created by FOIA requests are treated under the federal records laws in a manner similar to litigation holds, for which the FISA minimization procedures were amended. Under NARA regulations, for example, the "unlawful" destruction of records is defined to include the "disposal of a record subject to a FOIA request" in addition to records subject to litigation holds.[144]

---

141. H.R. REP. NO. 95-1283, pt. 1, at 56 (1978) (discussing destruction "where feasible"); *see also* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 9:5 (2016) (noting that with retention minimization "[o]utright physical destruction" is "not always necessary").

142. KRIS & WILSON, *supra* note 141, at § 9.5 (quoting legislative history).

143. *See, e.g.*, NSA SECTION 702 MINIMIZATION PROCEDURES, *supra* note 71, at 8 (requiring preservation of data "subject to a preservation obligation in pending or anticipated administrative, civil, or criminal litigation" while heightening restrictions on use and access). For FISA-related records that NARA has assessed to be of permanent value, similar restrictions on access or use as an alternative to destruction could potentially include transfer to NARA custody and control. *See supra* notes 106–10 and accompanying text. The Archivist is empowered for example to "accept for deposit" records the Archivist determines to "have sufficient historical or other value to warrant their continued preservation by the United States Government." 44 U.S.C. § 2107 (2012 & Supp. II 2015).

144. 36 C.F.R. § 1230.3(b) (2016).

Further, NARA-approved General Records Schedules provide for more lengthy retention periods for records subject to FOIA requests in order to reflect the statute of limitations for FOIA actions.[145]

Decades of FOIA litigation, in fact, provide a lengthy exercise in the interplay between the "right to know," national security and privacy concerns, relationships which evolve over time.[146] Classified information will eventually become declassified and the balance of privacy considerations often changes over time. In order for a FOIA requester to properly and fully satisfy their right to know, however, the records must survive.[147]

Finally, the Attorney General and NARA should ensure, at the very least, that minimization procedures incorporate a reference to federal records obligations in order to ensure compliance. In many cases, approved records schedules might already provide relevant approval. In other cases, however, a reference to record-keeping obligations would ensure that the issue is not overlooked and that the data and records at issue have been properly scheduled. Moreover, even if the surveillance data itself is destroyed, either due to minimization procedures or approved records schedules, NARA should aim to enhance accountability by ensuring that agencies heighten their documentation of the larger surveillance programs and the scope of the data being collected. This simply ensures compliance with the most basic statutory record-keeping duty—to "make and preserve" records that provide "adequate and proper documentation" sufficient to protect the legal rights of "persons directly affected by the agency's activities."[148]

---

145. *See* NARA, General Records Schedule 4.2, Information Access and Protection Records, at 49–50 (Jan. 2017), https://www.archives.gov/files/records-mgmt/grs/grs04-2.pdf (providing for a six-year retention period for FOIA case files including "copies of requested records").

146. The (b)(1) FOIA exemption protects properly classified information from public disclosure. 5 U.S.C. § 552(b)(1) (2012). Similarly, the (b)(6) FOIA exemption protects private information in circumstances in which privacy rights outweigh interests in public disclosure. *Id.* § 552(b)(6).

147. *See generally* Kissinger v. Reporters Comm. for Freedom of the Press, 445 U.S. 136, 139 (1980) (holding that FOIA only requires agencies to disclose agency records for which they have retained possession and control).

148. 44 U.S.C. § 3101 (2012). In doing so, NARA and agencies should consider the possibility of retaining representative samples to ensure a record of the type and extent of data collected on individuals.

CONCLUSION

In the end, it is possible that given all of the relevant complexities and conflicting incentives and the heightened dangers to privacy posed by advanced surveillance techniques, that the proper balance between privacy, security, and the "right to know" is not far off from the current state of affairs. What seems apparent, however, is that the intersection of these forces has not been directly and adequately confronted and addressed. The federal records laws are often overlooked, but the historic disclosures of sweeping government surveillance programs in recent years highlights the need for ensuring long-term accountability. The public controversy over these programs provides an opportunity to ensure that the balance is right, an opportunity that should not be squandered.

***