Chapter 1

AN OVERVIEW OF FEDERAL INFORMATION DISPUTES

1.1 THE PLAYERS IN FEDERAL INFORMATION DISPUTES 3
  1.1.1 Congress  3
  1.1.2 The courts  5
  1.1.3 Federal agencies  7
  1.1.4 Department of Justice  8
  1.1.5 Executive Office of the President  10
  1.1.6 National Archives and Records Administration  11

1.2 TRENDS IN FEDERAL INFORMATION LAW 13

On an average day, the U.S. government creates, collects, organizes, discloses, secures, and destroys millions of documents and other forms of information. It is impossible to know just how much information the federal government handles, but some isolated figures give an idea of the magnitude. For example, federal agencies maintain over 9,100 active forms, applications, and other types of information collections that solicit more than 84 billion responses annually from members of the public. The National Archives and Records Administration (the agency responsible for preserving significant federal records for future generations) houses over 2.8 million cubic feet of textual material and over 140 terabytes of electronic data. Countless other federal records are destroyed every day pursuant to general records schedules. In fiscal year 2010 alone, federal agencies made over 76.5 million decisions to classify federal information as either confidential,


secret, or top secret for reasons of national security,\(^3\) representing nearly a fivefold increase from fiscal year 2004.\(^4\) Although the specifics are not reported, each such classification decision likely encompasses multiple documents or pages of documents. Along with making all of these decisions, federal agencies received 597,415 requests for information from members of the public under the Freedom of Information Act (FOIA) in fiscal year 2010, up from 557,825 requests in 2009.\(^5\)

This book explains the legal framework that controls the federal government’s collection, management, and disclosure of its records. There is no single comprehensive statute that governs federal information. Instead, a patchwork of statutes, common law, regulations, executive orders, and judicial decisions governs the federal government’s handling of information. What law applies in any given situation depends on the entity that controls the information (e.g., Congress or an executive branch agency), what action that entity is taking (e.g., collecting, destroying, or disclosing information), and the nature of the information (e.g., personal privacy information, national security information, or confidential business information). There are several well-known statutes that dominate information disputes, such as the Freedom of Information Act.\(^6\) But the FOIA is just one of dozens of statutes governing federal information, and a given dispute may turn on a less familiar one like the Paperwork Reduction Act, the Classified Information Procedures Act, or a rider buried in an appropriations bill.\(^7\) Usually, several laws will apply.

Disputes over this federal information arise in a variety of contexts and involve many players. Businesses receive and respond to information requests from federal agencies conducting administrative investigations. Federal agencies make decisions daily about what information to release to individuals and organizations that make requests for information under

\(^6\) 5 U.S.C. § 552.
An Overview of Federal Information Disputes

the FOIA. Congress issues subpoenas for documents and testimony in the exercise of its legislative power. In civil litigation, government and private lawyers negotiate protective orders and argue over discovery requests for government information. Federal agencies make decisions to classify national security information, and those decisions are challenged by researchers, journalists, and other interested parties. Regulated entities submit comments in administrative rulemakings to dispute the quality of scientific information relied on by federal agencies.

Each of these disputes involves the same basic question: whether a given piece of information will be kept secret. In popular culture, the word “secret” has taken on a generally negative connotation. Secrets are bad; openness is good. Drilling down a little deeper, however, the matter is not that simple. Most Americans would agree that some level of secrecy is both necessary and desirable. The government must keep secret matters of national security. Businesses should have the right to keep secret their valuable and competitive information. Individuals should have the right to keep secret the details of their private lives. The policy question, then, is not whether there should be secrets but what types of information are entitled to secrecy and in what circumstances.

This book is not intended to draw the line between secrecy and openness in government in any particular place. Instead, this book is intended as a practical guide to assist practitioners facing the myriad situations involving access to information either from or by the federal government. The line between secrecy and openness will be drawn as each of those individual disputes is resolved.

1.1 THE PLAYERS IN FEDERAL INFORMATION DISPUTES

There are many entities within the three branches of the federal government that are frequently encountered in disputes over federal information. Understanding the legal authorities, policy objectives, and organizational structure of each is critical to successfully navigating a situation involving federal information.

1.1.1 Congress

Congress, of course, has the job of initiating and passing laws dealing with the collection, handling, and disclosure of government information. When subjecting other parts of government to burdensome information duties like those under the FOIA and the Paperwork Reduction Act (PRA), Congress
usually conveniently omits itself from coverage. In addition to passing legislation, Congress plays a significant oversight role with respect to agency information practices, such as through requirements for periodic reports or notices to Congress and through congressional requests for specific information from the agencies.

Congress often exercises its oversight responsibility with the help of the Government Accountability Office (GAO), Congress’s investigative agency. GAO was created in 1921 (then called the General Accounting Office) as an independent agency by the Budget and Accounting Act (the same statute that created the Bureau of Budget, later the Office of Management and Budget) and was given the job of overseeing the expenditure of federal funds. Beginning in the 1960s, Congress expanded GAO’s role beyond financial auditing and accounting and began asking the agency to perform more general evaluations of agency programs. This program-evaluation role results in a wide range of reports on federal agency information policy and practices that would not otherwise be available. The FOIA expressly authorizes and requires GAO to “conduct audits of administrative agencies on the implementation of [the FOIA] and issues reports detailing the results of such audits.”

GAO maintains that it, like Congress, is not subject to the FOIA and is therefore not obligated by that statute to release its records in response to a request from a member of the public. Nevertheless, GAO has volun-

8. See, e.g., 5 U.S.C. § 552(f) (defining “agency” for FOIA purposes to include only executive departments, government corporations, and independent regulatory agencies); 44 U.S.C. § 3502(1) (excluding Congress’s Government Accountability Office from PRA coverage); see also Banks v. Lappin, 539 F. Supp. 2d 228, 234 (D.D.C. 2008) (finding neither the House of Representatives nor the Senate to be an “agency” subject to the FOIA and the Privacy Act); United We Stand, Inc. v. Internal Revenue Serv., 359 F.3d 595, 597 (D.C. Cir. 2004) (“Because Congress is not an agency, congressional documents are not subject to FOIA’s disclosure requirement.”); Dow Jones & Co. v. Dep’t of Justice, 917 F.2d 571 (D.C. Cir. 1990) (holding that Congress is not covered by the FOIA).


10. 5 U.S.C. § 552(d) (“[The FOIA] is not authority to withhold information from Congress.”).


tarily adopted an information disclosure policy that includes some of the same principles as the FOIA. Under GAO’s policy, a person may submit a request for identifiable records of GAO. Nothing in the policy, however, obligates GAO to release the records, and the policy contains significant exclusions, including exclusions for records originating in another agency or nonfederal organization, records that are part of an ongoing review, and records related to work performed in response to a congressional request. If a federal agency wants to dispose of federal records related to claims against the United States prior to settlement of those claims, it must first obtain permission from GAO.

GAO’s ability to initiate litigation over federal records was diminished by a recent decision of the U.S. District Court for the District of Columbia. A case filed by GAO to obtain records relating to the National Energy Policy Development Group established by President George W. Bush and chaired by Vice President Cheney (the so-called Energy Task Force) was dismissed because the court concluded that the comptroller general lacked Article III standing.

1.1.2 The courts

The federal courts are often the final arbiters of disputes over federal information. Many information-related statutes grant jurisdiction to the federal courts to review agency decisions. For example, the FOIA makes an agency decision to withhold documents subject to review in federal district court. The Privacy Act authorizes four causes of action against federal agencies in federal district court, including two for money damages. Moreover, agency actions that do not fall within one of these specific statutes may be subject to review under the judicial review provisions of the Administrative Procedure Act (APA).

15. 4 C.F.R. pt. 81.
16. 4 C.F.R. § 81.4.
17. Id. §§ 81.5, .6(a).
21. Id. § 552a(g).
22. Id. § 706; see also Perkins v. Dep’t of Veterans Affairs, 572 F.3d 868 (11th Cir. 2009) (holding that requirements of the E-Government Act of 2002 and other information statutes were enforceable through the APA); McDonnell Douglas Corp. v. Widnall, 57 F.3d 1162 (D.C. Cir. 1995) (discussing “reverse FOIA” action under the APA).
Courts are also involved in the enforcement of administrative subpoenas by federal agencies that seek documents or other information from regulated parties. In civil litigation, courts rule on motions for protective orders in the context of discovery and on requests to quash or modify judicial subpoenas to protect, among other things, trade secrets and other confidential information. In criminal prosecutions, courts are also called on to enforce subpoenas and issue protective orders, and may be called on to manage classified information involved in the prosecution.

Among the federal courts, the District Court for the District of Columbia and the appellate court that reviews its decisions, the Court of Appeals for the District of Columbia Circuit, are frequent arbiters of disputes involving federal information. Thus, much of the case law on federal information law is generated by these courts. This is explained by the simple fact that many of the relevant statutory provisions that form the basis for court jurisdiction specifically permit venue in the District Court for the District of Columbia (regardless of the location of the disputed records) and that many federal agencies and their records are situated in that district, making venue permissible and convenient there. The frequency with which these two courts encounter federal information and other administrative law issues is often said to make them more sophisticated on these topics, thus making their precedent more persuasive to other federal district and circuit courts. However, other federal courts often define their own positions by disagreeing with the D.C. Circuit, and so a potential plaintiff would be advised to study the controlling law in the available courts before selecting a venue.

The Supreme Court considers federal information issues infrequently, so its 2010 term was unusual. The Court, in two separate decisions, narrowed the scope of two FOIA exemptions, thereby broadening the potential range and quantity of both private and government information that must be disclosed under the FOIA.

26. See section 4.5.
1.1.3 Federal agencies

Federal agencies, sometimes referred to as the fourth branch of government, are the primary collectors, handlers, destroyers, and disseminators of federal information. Agencies create information in the execution of their functions. Through their permitting, enforcement, and other regulatory activities, they gather a vast array of information from the private sector. Adequate and accurate information is critical to agency decision making, which is often reviewed by courts “on the record.” Laws such as the FOIA require that information in the control of these agencies, regardless of its source, be available to the public (subject to certain exclusions and exemptions). Both the Congress and the president are constantly involved in overseeing these agencies and attempting to control the type and quality of information they handle.

Although it is generally a simple matter to determine whether a particular government entity is an “agency,” the term is defined differently by different information statutes, and thus the coverage of these statutes will vary. For example, the FOIA and the Privacy Act define “agency” to include “any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.”

Based on the filing of annual FOIA reports, 15 federal departments and 82 other federal entities are subject to that statute. On the other hand, the PRA, while using the same general definition, expressly excludes, for example, the Government Accountability Office and the Federal Election Commission. Federal records-management statutes distinguish between an “executive agency” and a “federal agency” and include in the latter category “any executive agency or any establishment in the legislative or judicial branch of the government (except the Supreme Court, the Senate, the House of Representatives, and the Architect of the Capitol and any activities under the direction of the Architect of the Capitol).” Thus, when determining the information responsibilities of any particular governmental entity, the starting point is often the definition of “agency” in the relevant statutes and any case law interpreting those definitions.

31. **DOJ 2010 FOIA Summary, supra** note 5, at 1.
32. 44 U.S.C. § 3502(1); see also 44 U.S.C. § 3502(5) (definition of “independent regulatory agency”).
Within each agency, many information responsibilities are carried out by a chief information officer (CIO). This position was initially required by an amendment to the PRA,\textsuperscript{34} and subsequent statutes have added duties to be carried out by an agency’s CIO.\textsuperscript{35} The CIOs at federal agencies coordinate with each other through the Chief Information Officers Council.\textsuperscript{36} The council provides recommendations for government-wide information policy and guidance to CIOs to assist them in implementing their responsibilities.\textsuperscript{37}

Additionally, amendments to the FOIA in 2007 require each federal agency to designate a “Chief FOIA Officer.”\textsuperscript{38} The Chief FOIA Officer has several statutory duties, including “responsibility for efficient and appropriate compliance” with the FOIA and “monitor[ing] implementation of [the FOIA] throughout the agency.”\textsuperscript{39}

1.1.4 Department of Justice

The Department of Justice (DOJ) is subject to the FOIA and must disclose its agency records pursuant to that statute. However, DOJ possesses additional responsibilities under the FOIA that set it apart from other federal agencies. Perhaps most importantly, DOJ is given (nearly) exclusive authority to represent the United States, its agencies, and its officers in litigation.\textsuperscript{40} By virtue of this authority, DOJ is able to influence how other agencies exercise their obligations under the various information management and disclosure statutes, including the FOIA, often providing very specific guidance on what types of FOIA decisions DOJ will defend in court. Perhaps the


\textsuperscript{37} Id.; see also CHIEF INFO. OFFICERS COUNCIL, https://www.cio.gov (last visited May 31, 2013).

\textsuperscript{38} 5 U.S.C. § 552(j).

\textsuperscript{39} Id. § 552(k).

\textsuperscript{40} 28 U.S.C. §§ 516, 519; see also Marshall v. Gibson’s Products, Inc. of Plano, 584 F.2d 668, 676 n.11 (5th Cir. 1978) (“[T]he Attorney General is the chief legal officer of the United States. In this capacity and in the absence of an express congressional directive to the contrary, he is vested with plenary power over all litigation to which the United States or one of its agencies is a party.”). There are some exceptions to this exclusive grant of litigating authority. See, e.g., Tenn. Valley Auth. v. Envtl. Prot. Agency, 278 F.3d 1184, 1191–93 (11th Cir. 2002) (holding the Tennessee Valley Authority has independent litigating authority to maintain suit over objection of Attorney General), withdrawn in part, 336 F.3d 1236 (11th Cir. 2003).
An Overview of Federal Information Disputes

most notable of such guidance are memos now routinely issued by attorneys general setting forth their policy for defending decisions by federal agencies to exercise their discretion to withhold records from a FOIA requester.\(^{41}\) In addition, as an agency’s litigation counsel, DOJ lawyers will have final say over when to seek protective orders for documents produced in litigation or when to oppose such requests from other parties. The work done by DOJ and agency lawyers to search for and produce documents responsive to discovery requests in litigation has produced some noteworthy case law.\(^{42}\)

In addition, DOJ is required by statute to provide guidance to federal agencies for the preparation of their annual agency FOIA reports and to make those reports available electronically at a single access point.\(^{43}\) The Office of Information and Privacy is an office within DOJ whose job includes not only discharging DOJ’s obligations under the FOIA and the Privacy Act but also promoting agency compliance with the FOIA through developing and disseminating government-wide policy.\(^{44}\) The attorney general is charged with interpreting the provisions of the current executive order on classified information, if requested to do so by the head of an agency or the director of the Information Security Oversight Office.\(^{45}\)

DOJ also provides general guidance to agencies on FOIA and Privacy Act implementation, though this role may have been diminished somewhat by creation of the Office of Government Information Services within the National Archives and Records Administration in the 2007 FOIA amendments.\(^{46}\) Even so, DOJ continues to publish biannually its Guide to the Freedom of Information Act (DOJ FOIA Guide), which is an excellent and well-organized source of information that answers many questions about the FOIA and the Privacy Act. Private practitioners should be cautioned,

---

41. See, e.g., Memorandum from Eric Holder, Att’y Gen., to Heads of Executive Departments and Agencies (Mar. 19, 2009) (articulating and reinstating “foreseeable harm” standard for defending FOIA withholding decisions); Memorandum from John Ashcroft, Att’y Gen., to Heads of All Federal Departments and Agencies (Oct. 12, 2001) (articulating “sound legal basis” standard for defense of FOIA withholding decisions); Memorandum from Janet Reno, Att’y Gen., to Heads of Departments and Agencies (Oct. 4, 1993) (articulating “foreseeable harm” standard).


43. 5 U.S.C. § 552(e); see also Dep’t of Justice, Guidelines for Agency Preparation and Submission of Annual FOIA Reports, FOIA UPDATE, Summer 1997, at 3.


46. 5 U.S.C. § 552(h)(1).
however—sometimes the presentation of issues in the *DOJ FOIA Guide* can be slanted in the government’s favor. In fact, the *DOJ FOIA Guide* instructs agencies to ignore certain judicial decisions that are inconvenient to the government or otherwise contrary to its interests.\(^\text{47}\) It is, after all, the government’s guide. Courts, however, give no particular deference to agencies’ interpretation of the FOIA.\(^\text{48}\) Nevertheless, the *DOJ FOIA Guide* is a good starting point for research. Moreover, citation to it can be helpful in disputes with agencies at the administrative level, and DOJ would be hard-pressed to dispute a statement in its own guide during court litigation.

### 1.1.5 Executive Office of the President

The Executive Office of the President is a collection of offices and agencies within the White House. The FOIA provides that the Executive Office of the President is subject to the FOIA.\(^\text{49}\) However, courts have excluded from FOIA coverage “the President’s immediate personal staff or units in the Executive Office whose sole function is to advise and assist the President.”\(^\text{50}\) These FOIA-exempt components are referred to as the “White House Office.”\(^\text{51}\)

One part of the Executive Office of the President with significant responsibilities for information policy is the Office of Management and Budget (OMB). OMB was officially created in 1970 and inherited the functions of the Bureau of the Budget, created in 1921 as a part of the Treasury Department. The present-day responsibilities of OMB are, among other things, to assist in the development of the president’s annual budget submission to Congress and to assist the president in managing the executive branch departments and agencies. In this latter category falls OMB’s role in regulatory analysis and information management. This OMB function is carried out primarily by the Office of Information and Regulatory Affairs (OIRA). OIRA is an office within OMB created by the PRA.\(^\text{52}\) The Administrator of OIRA is appointed by the president with the advice and consent

---


49. 5 U.S.C. § 552(f).


52. 44 U.S.C. § 3503(a).
of the Senate and serves as the principal adviser to the director of OMB on federal information policy.\(^{53}\) OIRA reviews and approves information collection requests proposed by agencies under the PRA, implements the information quality requirements of the Information Quality Act and other laws, develops guidelines and policies on statistical activities of federal agencies, prepares reports to Congress on its funding of statistical activities, promulgates uniform fee schedules for FOIA requests, develops guidelines and regulations for use by federal agencies in carrying out the Privacy Act and other privacy statutes, and oversees federal agencies’ compliance with information technology security requirements.

### 1.1.6 National Archives and Records Administration

The National Archives and Records Administration (NARA) is an independent agency that oversees the management of the federal government’s records. Congress first established the National Archives as an independent agency in 1934\(^ {54}\) and later transferred the National Archives and its responsibilities to the General Services Administration.\(^ {55}\) The National Archives was again elevated to independent agency status in 1984, a status that it retains.\(^ {56}\) The head of NARA is the Archivist of the United States, who is appointed by the president with the advice and consent of the Senate.\(^ {57}\) Although it may come as a surprise to some, the position of Archivist can be a controversial one, sparking confirmation debate and opposition.\(^ {58}\)

NARA provides guidance and issues regulations applicable to agency records-management activities\(^ {59}\) and considers requests by federal agencies to destroy or otherwise dispose of agency records under the Federal Records Act.\(^ {60}\) NARA has the authority to inspect records and records-management practices of federal agencies.\(^ {61}\) NARA accepts for deposit into the National Archives records of federal agencies, Congress, and the Supreme Court that

\(^{53}\) 44 U.S.C. § 3503(b).

\(^{54}\) 48 Stat. 1122 (1934).


\(^{57}\) 44 U.S.C. § 2103(a).


\(^{60}\) 44 U.S.C. §§ 3105, 3302, 3303.

\(^{61}\) Id. § 2906(a)(1).
it determines “have sufficient historical or other value to warrant their con-
tinued preservation by the United States Government.” NARA is respon-
sible for the custody of records transferred to it and, upon transfer, assumes
the duty to carry out the permissive and restrictive statutory provisions that
applied to the head of the transferring agency with respect to the examina-
tion and use of those records. NARA plays a role in the decision to dispose
of presidential records during the president’s term of office and assumes
responsibility for the custody and preservation of presidential records upon
conclusion of a president’s term. NARA is charged with providing guid-
ance to federal agencies regarding federal information on the Internet and
other electronic records. NARA publishes, among other things, the Fed-
eral Register, the Code of Federal Regulations, the Weekly Compilation
of Presidential Documents, and the U.S. Statutes at Large.

The 2007 amendments to the FOIA gave NARA a larger role in FOIA
implementation. The amendments created the Office of Government Infor-
mation Services within NARA. Its duties include “review[ing] policies
and procedures of administrative agencies under [the FOIA]” and reviewing
agency compliance with the FOIA. It also is required to offer mediation
services to resolve FOIA disputes between FOIA requesters and agencies as
an alternative to litigation.

The Information Security Oversight Office (ISOO) is a component of
NARA that plays an important oversight and advisory role in the process of
classifying and declassifying information. By virtue of executive order, the
director of ISOO may determine that information has been improperly clas-
sified and, in response, order the agency that originated the classification to
declassify the information. The director of ISOO is also responsible for
issuing binding directives to federal agencies to implement the president’s
executive order on classification. The director of ISOO oversees agen-
cies’ classification activities, reviews and approves agency regulations and

62. Id. § 2107(1).
63. Id. § 2108(a).
64. Id. §§ 2201–2207.
67. Id.
68. 5 U.S.C. § 552(h).
69. Id. § 552(h)(2).
70. Id. § 552(h)(3).
72. Id. § 5.1.
guides regarding automatic declassification review, and may conduct on-site inspections of agency classification programs.\textsuperscript{73}

1.2 TRENDS IN FEDERAL INFORMATION LAW

Most disputes over federal information are routine everyday occurrences. Many disputes, however, have great significance for one or more reasons. Some disputes are subplots in high-profile political matters. When Secretary of State Henry Kissinger left the State Department and took records from his office with him, he was sued for return of the records.\textsuperscript{74} The suicide of Vincent Foster, deputy counsel to President Clinton, produced a dispute over access to photographs of his death scene and resulted in Supreme Court precedent about the scope of the FOIA’s exemption for personal privacy information.\textsuperscript{75} Linda Tripp, former federal employee and confidant of Monica Lewinsky, sued the Department of Defense for releasing information relating to her application for federal employment.\textsuperscript{76} The prosecution of Zacarias Moussaoui, accused September 11 would-be hijacker, brought attention to the difficulties of handling classified national security information in a criminal prosecution.\textsuperscript{77} Disputes over federal information are often surrogates for larger policy or substantive disputes. For instance, environmental groups sued Vice President Cheney for access to the records of his Energy Task Force in an effort to prove that the task force recommendations on energy policy were generated by representatives of the energy industry.\textsuperscript{78} Recently, Congress has sought access to e-mails of the Environmental Protection Agency’s Administrator and other top officials in the Obama administration that were sent and received under aliases and through private e-mail accounts, claiming the use of such accounts violates the Federal Records Act.\textsuperscript{79} The practice of using information law obligations to achieve substantive policy objectives is certain to continue.

Federal information law also frequently raises issues about separation of powers in very practical and concrete settings. For example, to what

\textsuperscript{73} Id. § 5.2(b)(2)–(4).
\textsuperscript{77} United States v. Moussaoui, 333 F.3d 509 (4th Cir. 2003).
Chapter 1

extent can the legislative branch assert ownership and control over presidential records after a president leaves office? Does the executive branch have the authority to classify federal information as secret absent any legislative authorization? Can Congress require the federal courts to adopt rules about public access to court records? On these and other questions, the three branches have managed to strike a delicate balance between vigorously asserting their roles under the Constitution and compromising (without saying so) to avoid constitutional crisis.

Information law and policy have always been responsive to contemporary events (the Privacy Act was born in the aftermath of Watergate and concerns over government eavesdropping). Today, the two most powerful drivers of federal information law and policy are advances in information technology and concerns about homeland security. The federal government is increasingly collecting, organizing, securing, and preserving information electronically. At the same time, the Internet is making this federal information available to the public more quickly. The war on terror pulls in multiple directions—for example, expanding the amount of information that is collected and shared by federal agencies, while also constricting the amount of information that is publicly available. Despite these strong contemporary forces, legal and policy changes with respect to federal information take place against a backdrop of constitutional, statutory, and common law principles that have been in existence for decades or longer. Understanding this legal backdrop is key to making sense of current and future changes.

80. S. REP. NO. 93-1183, REPRINTED IN 1974 U.S.C.C.A.N. 6916 (1974) (“[The Privacy Act] is designed to prevent the kind of illegal, unwise, overbroad, investigation and record surveillance of law-abiding citizens produced in recent years from actions of some over-zealous investigators, and the curiosity of some government administrators, or the wrongful disclosure and use, in some cases, of personal files held by Federal agencies.”).