The Ohio State Technology Law Journal

PRIVACY EXCEPTIONALISM UNLESS IT'S UNEXCEPTIONAL: HOW THE AMERICAN GOVERNMENT MISUSES THE SPIRIT OF PRIVACY IN TWO DIFFERENT WAYS TO JUSTIFY BOTH NONDISCLOSURE AND SURVEILLANCE

BENJAMIN W. CRAMER*

CONTENTS

* Associate Teaching Professor, Donald P. Bellisario College of Communications, Pennsylvania State University.

I. Introduction

The Freedom of Information Act (FOIA)[1] has two exemptions—Exemption 6[2] and Exemption 7(C)[3]that specifically allow a requested document to be withheld to protect the privacy of persons named within. For the first two decades of FOIA's history, the use of those two exemptions by Executive Branch agencies was not particularly notable. This changed with the *Reporters Committee* ruling by the Supreme Court in 1989 on the concerns of people named in government-held documents.[4] Since then, scholars have examined the growing trend of *privacy exceptionalism* in agency denials of requests for documents under FOIA. As Martin Halstuk[5] and others[6] have

---

[1] 5 U.S.C. § 552 (2016).

[2] 5 U.S.C. § 552(b)(6) (2016) (allowing the withholding of "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy").

[3] 5 U.S.C. § 552(b)(7)(C) (2016) (allowing the withholding of law enforcement-related documents that "could reasonably be expected to constitute an unwarranted invasion of personal privacy").

[4] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989). This ruling will be discussed in detail at *infra* notes 21-28 and accompanying text.

[5] *See, e.g.*, Martin E. Halstuk, *Blurred Vision: How Supreme Court FOIA Opinions on Invasion of Privacy Have Missed the Target of Legislative Intent*, 4 COMM. L. & POL'Y 111 (1999); Martin E. Halstuk, *Policy of Secrecy - Pattern of Deception: What Federalist Leaders Thought about a Public Right to Know*, 1794-98, 7 COMM. L. & POL'Y 51 (2002); Martin E. Halstuk, *Shielding Private Lives from Prying Eyes: The Escalating Conflict Between Constitutional Privacy and the Accountability Principle of Democracy*, 11 COMMLAW CONSPECTUS 71 (2003); Martin E. Halstuk, *When Is an Invasion of Privacy Unwarranted Under the FOIA? An Analysis of the Supreme Court's "Sufficient Reason" and "Presumption of Legitimacy" Standards*, 16 U. FLA. J.L. & PUB. POL'Y 361 (2005).

[6] *See, e.g.*, Micah Altman, Alexandra Wood, David R. O'Brien, Salil Vadhan & Urs Gasser, *Towards a Modern Approach to Privacy-Aware Government Data Releases*, 30 BERKELEY TECH. L.J. 1967 (2015); Clay Calvert, Austin Vining, & Sebastian Zarate, *Reining in Internet-Age Expansion of Exemption 7(C): Towards a Tort Law Approach for Ferreting out Legitimate Privacy Concerns and Unwarranted Intrusions Under FOIA*, 70 SMU L. REV. 255 (2017); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013); Kathryn Shephard, *Mug Shot Disclosure Under FOIA: Does Privacy or Public Interest Prevail*, 108 NW. U. L. REV. 343 (2013).

shown, the *Reporters Committee* precedent has enabled agencies to deny FOIA requests for documents to protect the supposed privacy rights of any person whose name appears therein, even if they are not relevant to the document's topic. Thus, a trend has emerged in FOIA jurisprudence in which someone's personal privacy has become more *exceptional*[7] than the information on governmental operations to be found within the requested documents. This trend in document disclosure practices gives the impression that the American government cares deeply about the personal privacy of individuals named in sensitive documents that could be perused by strangers if agencies hand them over to requesters. In fact, even as the government claims that privacy should be safeguarded when someone requests a document, researchers have located some absurd examples of this practice being used to justify agency secrecy.[8]

---

[7] The concept of *privacy exceptionalism* in FOIA privacy disputes was first developed, though not under that particular name, in Michael Hoefges, Martin E. Halstuk & Bill F. Chamberlin, *Privacy Rights Versus FOIA Disclosure Policy: The "Uses and Effects" Double Standard in Access to Personally Identifiable Information in Government Records*, 12 WM. & MARY BILL RTS. J. 1 (2003). The term *privacy exceptionalism* was first defined precisely, in the context of the *Reporters Committee* ruling and its aftermath, in Martin E. Halstuk, Pa. State Univ., Benjamin W. Cramer, Pa. State Univ., and Michael D. Todd, Univ. of N.H., Public Interest…what Public Interest? How the Rehnquist Court Created the FOIA Privacy Exceptionalism Doctrine, Paper Presented at the Association for Education in Journalism and Mass Communication Annual Conference (Aug. 12, 2012).

[8] The absurd uses of privacy to deny requests for government-held documents range from the comical to the tragic. For example, in 2002 the National Zoo in Washington, D.C. denied the *Washington Post* access to the medical records of a giraffe that had died, on the grounds that disclosure would violate the dead animal's privacy rights. *See* National Zoo Asserts Animal Privacy, ACCESS REP., May 8, 2002, at 9. In 2011, the Federal Communications Commission refused to disclose documents on how a telephone company handled thousands of dollars of taxpayer money because the documents contained the name of a company employee whose privacy was apparently at risk. *See* Benjamin W. Cramer, *Privacy Exceptionalism and Confidentiality Versus the Public Interest in Uncovering Universal Service Fraud*, 20 COMM. L. & POL'Y 149, 170-71 (2015). On the more tragic side, in the 1980s the U.S. Department of State refused to release the names of Haitian refugees for reasons of privacy, even though activists were prepared to shield those persons from persecution in their homeland. This resulted in the Supreme Court case U.S. Dep't of State v. Ray, 502 U.S. 164 (1991), which will be discussed in detail at *infra* notes 45-46 and accompanying text.

And, even if the American government truly cares about a citizen's personal privacy, its attitudes and practices in other realms of governance suggest the opposite. As seen in the Edward Snowden revelations of 2013[9] and subsequent political controversies,[10] any governmental claim that it wishes to protect citizens' personal privacy has become nonsensical, if not downright farcical. Outside of documents withheld from disclosure under FOIA Exemptions 6 and 7(C), evidence indicates that the American government at large now views personal privacy as inherently *unexceptional*, or not nearly important enough to overcome the demands of the rapidly-spreading surveillance state.[11] As opposed to the *privacy exceptionalism* detected by scholars in the use of FOIA Exemptions 6 and 7(C), the surveillance state has enabled a contradictory trend of *privacy unexceptionalism*.

---

[9] This heavily reported event was first reported by journalist Glenn Greenwald; for a summary of his early reports, see generally GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014).

[10] The desire of the national security establishment to collect citizens' personal communications records has mutated into (among other things) demands for tech companies to de-encrypt communications and calls for Executive Branch authority to restrict the use of telecommunications systems and the Internet during emergencies. *See, e.g.*, Scott M. Ruggiero, *Killing the Internet to Keep America Alive: The Myths and Realities of the Internet Kill Switch*, 15 SMU SCI. & TECH. L. REV. 241, 241-42 (2012); Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (March 28, 2016), https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html [https://perma.cc/YU5Y-UHD3].

[11] *See, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008); Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773 (2015); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309 (2012); Joel R. Reidenberg, *The Data Surveillance State in the United States and Europe,* 49 WAKE FOREST L. REV. 583 (2014); Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014); Eric M. Yesner, *Government Surveillance Through New Technology: Rethinking the Third-Party Doctrine's Implications on the Fourth Amendment*, 19 HOLY CROSS J.L. & PUB. POL'Y 135 (2015).

This article will explore the American government's contradictory stances toward personal privacy, via an analysis of the jurisprudence surrounding FOIA and the Privacy Act of 1974,[12] while comparing that to surveillance-oriented jurisprudence surrounding the actions of various agencies in the national security and law enforcement establishments. Furthermore, the article will argue that this contradiction is not just a matter of defining values, but it also allows the government to violate the spirit of government transparency and the value of privacy in two different ways while becoming more secretive across the board.

The next section of this article will review the jurisprudence surrounding Exemptions 6 and 7(C) of FOIA, and the trends that have resulted in judicial deference toward agency rejections of FOIA requests for often facetious reasons of personal privacy—what researchers have dubbed *privacy exceptionalism*. The third section will perform a similar analysis of the Privacy Act of 1974 as another example of the American government's professed concern for protecting personal privacy through document management practices.

The fourth section of the article will review how the national security and law enforcement establishments have largely disdained or ignored personal privacy as it conducts antiterrorism investigations and widespread electronic surveillance of citizens, in ways that contradict the agencies' own statements on privacy protections and also contradict the rest of the American government's supposed concerns about privacy as a reason to reject requests for documents. In that section, the evidence will point to a new type of *privacy unexceptionalism*, because privacy values have been unable to overcome the excesses of the surveillance state, and because the surveillance state ignores those values altogether. The article will conclude with a discussion of the contradictions between these two views of privacy in the American government, and the possible ramifications for civil liberties when citizens seek information about governmental operations or object to the tracking of their personal data.

---

[12] 5 U.S.C. § 552a (2014).

II. Privacy Exceptionalism in FOIA Jurisprudence

Upon its passage in 1966, FOIA included two privacy provisions at Exemptions 6 and 7(C), which can be cited by executive branch agencies to deny a FOIA request for documents. However, there was no indication that Congress intended document disclosure to be trumped by privacy values in any significant way, and such a thing did not happen in any notable fashion before 1989.[13] Exemption 6 allows government agencies to withhold "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[14] During debates on the need for Exemption 6, the U.S. Senate stated that this exemption should maintain a balance between the "protection of an individual's private affairs from unnecessary public scrutiny, and the preservation of the public's right to governmental information."[15]

Meanwhile, Exemption 7(C) works in a similar fashion but pertains specifically to the documents compiled during a law enforcement investigation. This exemption operates under the belief that the persons named in such documents could face harm from the disclosure of their identities, or that disclosure could hamper the investigation.[16] The text of Exemption 7(C) requires the government agency to prove that disclosure could "reasonably be expected" to constitute an invasion of privacy that would threaten a named individual's safety.[17] Exemption 7(C) was intended to favor personal privacy more strongly than Exemption 6, thanks to the sensitivity of law enforcement investigations, but agencies were still required to weigh that privacy

---

[13] Martin E. Halstuk & Charles N. Davis, *The Public Interest Be Damned: Lower Court Treatment of the Reporters Committee "Central Purpose" Reformulation*, 54 ADMIN. L. REV. 983, 1021 (2002).

[14] 5 U.S.C. § 552(b)(6) (2016). Congress wrote this exemption to include "personnel and medical files" but noted that these were only meant to be examples of possible categories and were not meant to exclude other categories of information that could be considered private. *See* H.R. REP. NO. 89-1497, at 11 (1966).

[15] *See* S. REP. NO. 89-813, at 9 (1965).

[16] 5 U.S.C. § 552(b)(7)(C) (2016).

[17] *Id*.

against the public interest in the other information to be found in the requested documents.[18]

This proposed balance of interests indicates that Congress did not intend for privacy rights, through abuse or overuse of FOIA Exemptions 6 or 7(C), to easily overcome public knowledge of governmental operations.[19] Initially, a government agency that denied a FOIA request for reasons of personal privacy carried the burden of proof in showing that the concerns of the private individual named in the document outweighed the public interest in disclosure.[20]

The turning point on this matter was the *Reporters Committee* ruling of 1989,[21] at which time the Supreme Court constructed—"out of whole cloth" in the later estimation of the plaintiffs[22]—a previously non-existent "central purpose [of FOIA] . . . to ensure that the Government's activities be opened to the sharp eye of public scrutiny, not that information about private citizens that happens to be in the warehouse of the Government be so disclosed."[23] This was an abrupt departure from previous FOIA practice.

The *Reporters Committee* case arose when television reporter Robert Schakne filed a FOIA request for FBI records on Charles Medico, who was involved with a mob-dominated company that in turn was under investigation for its connection to a bribery scandal surrounding former U.S. Representative Daniel Flood.[24] While the FBI disclosed

---

[18] *See* H.R. REP. NO. 109-226, at 18 (2005).
[19] *See* Hoefges, Halstuk & Chamberlin, *supra* note 7, at 13.
[20] *See, e.g.*, Aronson v. U.S. Dep't of Hous. & Urban Dev., 822 F.2d 182, 187-88 (1st Cir. 1987) (rejecting a vague government justification for withholding data on private persons); Sterling Drug, Inc. v. Fed. Trade Comm'n, 450 F.2d 698, 703-05 (D.C. Cir. 1971) (holding that the burden of justifying nondisclosure must be met by the government).
[21] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989).
[22] *See* Brief for the Reporters Comm. for Freedom of the Press et al. as Amici Curiae Supporting Respondents at 11, Office of Indep. Counsel v. Favish, 541 U.S. 157 (2004) (no. 02-954).
[23] *Reporters Comm.*, 489 U.S. at 774 (emphasis removed).
[24] *Id.* at 757.

some of the requested records, it withheld others under the rationale that they invaded Medico's privacy.[25] After an 11-year court battle between Reporters Committee for Freedom of the Press and the Department of Justice, the Supreme Court ruled that when requesting documents in which private persons are named for virtually any reason, the requester is required to provide evidence that the public interest in the documents outweighs the personal privacy interest of the persons named within.[26]

According to Justice John Paul Stevens, FOIA's "central purpose" was to enlighten citizens about the workings of government, not to expose the private affairs of individuals,[27] and in this particular case, the Court determined that the requested rap sheets on Medico would not educate the public on the workings of the FBI or the Congressman that the reporter was investigating.[28]

Before *Reporters Committee*, in the words of Halstuk and Davis, "courts routinely held that the FOIA can be used for any private or public purpose, without the need for a requester [to] be required to justify a request."[29] But after *Reporters Committee*, whenever a government agency denies a FOIA request by citing personal privacy, the requester now has the very difficult and often impossible task of proving that the public interest in the information on governmental operations found in the documents will outweigh the privacy interest of persons named within; and paradoxically, the requester must often make this argument without even seeing the documents in question because the FOIA request is still being processed.[30] This is the result of the previously unknown "central purpose" of FOIA as created by Justice Stevens in the ruling. Stevens's future Supreme Court colleague Ruth Bader Ginsburg later noted that this requirement is not

---

[25] *Id*. This withholding decision cited FOIA Exemption 7(C), protecting the privacy of persons mentioned in documents related to law enforcement investigations. 5 U.S.C. § 552(b)(7)(C) (2016).
[26] *See* Halstuk & Davis, *supra* note 13, at 989–90.
[27] *Reporters Comm*., 489 U.S. at 775.
[28] *Id*. at 774.
[29] *See* Halstuk & Davis, *supra* note 13, at 1021.
[30] *See* Cramer, *supra* note 8, at 183.

found in the statutory language of FOIA, and that the *Reporters Committee* ruling "changed the FOIA calculus."[31]

The *Reporters Committee* ruling enabled an explosion of FOIA denials for reasons of personal privacy, with agency usage of Exemptions 6 and 7(C) increasing by leaps and bounds ever since, with little evidence that the trend will slow down anytime soon.[32] Also, Exemptions 6 and 7(C) are now often cited simultaneously in agency denials of FOIA requests for documents—with Exemption 6 being used as a catch-all justification to withhold a document containing the name of any individual person, regardless of that person's notability for the governmental operations discussed in the document; and with Exemption 7(C) being used to justify an expansive definition of "law enforcement" into myriad matters of national security and antiterrorism.[33]

The "central purpose" test that the Supreme Court created out of whole cloth in the *Reporters Committee* ruling, requiring that requesters prove in court that their requested documents can fulfill the supposed central purpose of FOIA to provide illumination on matters of the public interest, has dramatically narrowed the scope of records available to citizens via FOIA request.[34] Lower courts have generally adopted the "central purpose" test to conclude that document requesters must prove that the documents directly shed light on a government agency's performance, and if not, then they do not justify

---

[31] U.S. Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 505–07 (1994) (Ginsburg, J., concurring).

[32] *See* Martin E. Halstuk, Benjamin W. Cramer & Michael D. Todd, *Tipping the Scales: How the U.S. Supreme Court Eviscerated Freedom of Information in Favor of Privacy*, *in* TRANSPARENCY 2.0: DIGITAL DATA AND PRIVACY IN A WIRED WORLD 16, 20-24 (Charles N. Davis & David Cuillier eds., 2014).

[33] *Id*. The expansion of the FOIA law enforcement exemptions being used to justify a growing range of practices that were previously considered to be national security, and not necessarily law enforcement, will be discussed later in this article. *See infra* Section IV.

[34] *See* Halstuk & Davis, *supra* note 13, at 997.

the invasion of privacy for any person named therein, regardless of the utility of any of the other information presented in the document.[35]

Before the advent of the "central purpose" test, the federal courts, when addressing privacy-related FOIA denials, generally performed an analysis that balanced the privacy interests of the individual against the public interest in disclosure, with each having a roughly equal chance of success.[36] According to Halstuk and Davis, the *Reporters Committee* ruling brought an unceremonious end to this type of analysis, and since 1989 there has been a "blanket denial of nearly all requests for lists of names because such records fall beyond the 'central purpose' of the FOIA, and also the end of any sort of judicial reflection of the potential benefits of disclosure."[37]

Reporters Committee and two similar Supreme Court holdings on the importance of personal privacy over the public interest in obtaining government-held documents—*Department of State v. Washington Post Co.*[38] and *National Records and Archives Admin. v. Favish*[39]—are primarily responsible for a rapidly-expanding trend in which the courts

---

[35] *See, e.g.*, Accuracy in Media, Inc. v. Nat'l Park Serv., 194 F.3d 120, 123 (D.C. Cir. 1999) (ruling that the release of autopsy photographs is an invasion of privacy for the deceased person pictured or his/her relatives); Comput. Prof. for Soc. Resp. v. Secret Serv., 72 F.3d 897, 904 (D.C. Cir. 1996) (ruling that the requester must offer compelling evidence of agency misconduct, and prove that this misconduct outweighs the privacy rights of named individuals, before receiving law enforcement-related documents). Note that the "central purpose" concocted by Justice Stevens in *Reporters Committee* is sometimes called the "core purpose" in later rulings.

[36] *See* Halstuk & Davis, *supra* note 13, at 1001-02. This technique was first formulated by the Supreme Court in Dep't of the Air Force v. Rose, 425 U.S. 352, 353-54 (1976) (allowing researchers to access the academic and disciplinary records of students at the Air Force Academy).

[37] *See* Halstuk & Davis, *supra* note 13, at 1002.

[38] U.S. Dep't of State v. Wash. Post Co., 456 U.S. 595, 601-03 (1982) (ruling that government-held records on Iranian nationals living in the United States, during a period of extensive strife between the two nations, would violate those persons' privacy).

[39] Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 173-75 (2004) (ruling that crime scene photographs can be withheld to protect the personal privacy of the victim's family, despite public interest in the victim and in the crime itself).

uphold agency FOIA denials for reasons of privacy, with little regard for other arguments.[40] Particularly since the *Reporters Committee* and *Washington Post* rulings—both in the 1980s—the effectiveness of FOIA has been hampered by attempts to protect the privacy of individuals named in documents regardless of the public interest in governmental operations described in those same documents.[41] Excessive use of such exemptions by agencies, as enabled by these Supreme Court precedents, has led one Congressional committee to declare that "FOIA . . . is broken."[42]

The use of the FOIA privacy exemptions by government agencies to withhold documents has resulted in many questionable conclusions on the value of personal privacy, with the U.S. Department of Justice complaining that even the presence of non-intimate personal information could justify withholding a requested document.[43] Also, the Supreme Court has neglected to provide any detailed listing of the types of information that should (or should not) justify withholding a document on privacy grounds, thus allowing agencies to decide what is "private."[44]

In one of the more absurd post-*Reporters Committee* rulings on this matter, the Supreme Court refused to overturn a FOIA rejection by the State Department concerning information on Haitian refugees who had

---

[40] *See* A. Jay Wagner, *A Secret Police: The Lasting Impact of the 1986 FOIA Amendments*, 23 COMM. L. & POL'Y 387, 414 (2018).
[41] *See* Tyler Prime & Joseph Russomanno, *The Future of FOIA: Course Corrections for the Digital Age*, 23 COMM. L. & POL'Y 267, 270 (2018).
[42] Staff Of H.R. Comm. on Oversight and Gov't Reform, 114th Cong., FOIA is Broken: A Report 39 (2016), https://republicans-oversight.house.gov/wp-content/uploads/2016/01/FINAL-FOIA-Report-January-2016.pdf. For an executive summary, see Christopher J. Walker, *FOIA Is Broken: New Chaffetz House Oversight Committee Report*, YALE J. ON REG.: NOTICE & COMMENT (Jan. 14, 2016), http://yalejreg.com/nc/foia-is-broken-new-chaffetz-house-oversight-committee-report-by-chris- walker/ [https://perma.cc/FJH2-6VY9].
[43] Office of Info. and Privacy, U.S. Dep't of Justice, A 325-27 (Pamela Maida ed., 2002).
[44] *See* Lillian R. BeVier, *Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 490 (1995).

fled to America in the 1980s. Supporters of these refugees requested information on whether any of them were being considered for deportation back to Haiti, in the fear that they would then be persecuted by that country's ruling regime. The agency denied the request under FOIA Exemption 6 because the personal privacy of the individuals named would be violated. Their privacy interests apparently outweighed real evidence of physical danger and the efforts of activists to find out who they were in order to protect them. The Supreme Court agreed with this reasoning, stating that "mere speculation about hypothetical public benefits cannot outweigh a demonstrably significant invasion of privacy,"[45] The Court also suggested that there had to be some evidence that the general public beyond just the requesters would find the documents worthwhile.[46]

That final point about the general public was reaffirmed by the Supreme Court in a later ruling that supported the withholding of employment documents by the Federal Labor Relations Authority. Here, the Court emphasized that "the *only* relevant public interest in the FOIA [privacy] balancing analysis [is] the extent to which disclosure of the information sought would shed light on an agency's performance of its statutory duties or otherwise let citizens know what their government is up to."[47] Again, this requires requesters to prove the public interest value of documents that they have not yet seen. Since *Reporters Committee*, the Supreme Court has not ruled in favor of the disclosure of documents in a FOIA dispute in which agencies invoked the privacy exemptions, and is unlikely to do so as long as any comparison of the privacy interest versus public interest is framed via the "central purpose" doctrine from that ruling.[48]

---

[45] Dep't of State v. Ray, 502 U.S. 164, 179 (1991).
[46] *See id*. at 178.
[47] Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 497 (1994) (emphasis added) (some internal quotation marks omitted). In this case, a labor union requested agency-held documents on union members in order to gather information it felt was reasonably necessary for collective bargaining purposes. *Id*. at 488-90. The requested documents included addresses, and similar information, so the agency denied the request under FOIA Exemption 6. *Id*. at 488.
[48] *See* Cramer, *supra* note 8, at 183-84. Note that the "central purpose" doctrine has occasionally been criticized by the judiciary for its restrictive nature and for

The public interest is now at an automatic disadvantage when it conflicts with privacy in a FOIA dispute,[49] and there is evidence that agencies may be tempted to over-invoke the FOIA privacy exemptions to deny document requests, with less worry of being overturned by the courts.[50] By 2000, Exemption 6 had become the most commonly used exemption at federal agencies to justify FOIA denials, with Exemption 7(C) in a close second. All other exemptions were significantly behind.[51] By 2017, the most recent year for which records were available at the time of writing, Exemptions 6 and 7(C) were still the two most frequently used, with evidence that they are also frequently used together.[52]

Harold L. Cross, who advised Congress on the development and passage of FOIA, made a forceful statement on why citizens should know what their government is doing: "Public business is the public's business. The people have the right to know. Freedom of information

---

the fact that it was not present in previous FOIA jurisprudence, though without tipping any ruling toward disclosure. *See, e.g.*, Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. at 507 (O'Connor, J., concurring).

[49] *See* Robert Gellman, *Public Records – Access, Privacy, and Public Policy: A Discussion Paper*, 12 GOV'T INFO. Q. 391, 391 (1995).

[50] *See* Cramer, *supra* note 8, at 182.

[51] U.S. Dep't of Justice, DOJ FOIA 2000 ANNUAL REPORT – OTHER REASONS FOR NONDISCLOSURE, https://www.justice.gov/oip/doj-foia-2000-annual-report-other-reasons-nondisclosure [https://perma.cc/DZ4H-2V6U].

[52] *See* U.S. DEP'T OF JUSTICE, ANNUAL FREEDOM OF INFORMATION ACT REPORT FISCAL YEAR 2017 § V.B.(3) (2018), https://www.justice.gov/oip/page/file/1024596/download. During fiscal year 2017, Exemption 6 was used 9,239 times to reject FOIA requests and Exemption 7(C) was used 9,286 times. One of the other law enforcement exemptions, 7(E), was in a distant third place at 4,809 uses. *Id.* Exemption 7(E) allows the withholding of documents that "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552 (b)(7)(E) (2016). Exemptions 6 and 7(C), both dealing with privacy, are typically used in tandem and their separate meanings are often intertwined when used by agencies to justify FOIA denials. Either of these exemptions, and frequently both together, are cited in at least three-fifths of FOIA denials by agencies in recent years. *See* Prime & Russomanno, *supra* note 41, at 288; Wagner, *supra* note 40, at 414, 421.

is their just heritage. Without that the citizens of a democracy have but changed their kings."[53] This philosophy still occasionally appears in FOIA jurisprudence; for example, the Supreme Court asserted in 2004 that government transparency is "a structural necessity in a real democracy" and that access to documents provides a "means for citizens to know what the Government is up to."[54] Unfortunately, this standard has withered away when those documents contain personal information, however slight or inconsequential it may be.

III. The Spirit of the Privacy Act of 1974

The Privacy Act of 1974[55] was passed at a time of growing Congressional concern about the increasing sophistication and pervasiveness of computers and databases that could gather personal information on American citizens.[56] As opposed to the pro-disclosure philosophy of FOIA, the Privacy Act compels government agencies to withhold records that contain personal information.[57] In an ironic (or perhaps Machiavellian) twist, the Privacy Act was the outcome of a federal governmental inquiry on privacy rights convened by President Richard Nixon in early 1974, when he was under investigation for widespread violations of those same rights.[58]

The Privacy Act was meant to temper the widespread disclosure of records containing personal information that was enabled by the passage of FOIA eight years earlier.[59] However, it is important to the

---

[53] HAROLD L. CROSS, THE PEOPLE'S RIGHT TO KNOW, at XIII (1953).
[54] Nat'l Archives & Records Admin. v. Favish, 541 U.S. 157, 160 (2004).
[55] 5 U.S.C. § 552a (2014).
[56] *See, e.g.*, S. REP. NO. 93-1183, at 7–8 (1974); H.R. REP. NO. 93-1416, at 3, 7–8 (1974).
[57] Corizarek, *Reconciling FOIA and the Privacy Act, National Archives: FOIA Ombudsman, OGIS* (Oct. 26, 2012), https://foia.blogs.archives.gov/2012/10/26/reconciling-foia-and-the-privacy-act/ [https://perma.cc/H8VJ-CBK6].
[58] *See* Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199, 211-13 (1993).
[59] *See* Robert E. Gregg, *The Privacy Act of 1974*, ARMY LAW., July 1975, at 25, 26, 29.

note that the Privacy Act does not enforce any sort of *right* to privacy. Unlike the pro-disclosure and anti-secrecy philosophy of FOIA, which was based on centuries of democratic theory and the Founding Fathers' distrust of centralized government,[60] there is much less support for a right to privacy in America. Such a right was first proposed in an influential but exploratory article by Warren and Brandeis in 1890,[61] but by the early 1970s the "right to privacy" (which is not mentioned in the Constitution) had only been cobbled together by the Supreme Court into an *implied* right through creative interpretations of the First, Third, Fourth, Fifth, and Fourteenth Amendments.[62]

Also in the early 1970s, electronic surveillance, which does not require physical intrusion by law enforcement officers, inspired a renewed call for some sort of privacy protection for the common citizen, probably in the form of a statutory protection.[63] Around that time there had been proposals for the establishment of a "National Data Center" to collect and store personal information on citizens in the interests of countering Communist intrusion and other supposed Cold War threats, which worried privacy advocates.[64] Privacy statutes focused on precise categories of information began to appear, starting with the Fair Credit Reporting Act of 1970.[65]

---

[60] *See* Jerome J. Hanus & Harold C. Relyea, *A Policy Assessment of the Privacy Act of 1974*, 25 AM. U.L. REV. 555, 559-61 (1976).
[61] *See* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 197 (1890).
[62] *See* Roe v. Wade, 410 U.S. 113, 152-53 (1973); Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965). The Supreme Court had also suggested that the Fourth Amendment, which is typically viewed as a procedure for law enforcement officials to obtain a warrant before searching through a citizen's personal effects, could be viewed as an indirect or implied right to privacy, though this conception was not dispositive to each case's disputes over police procedures. Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting); Boyd v. United States, 116 U.S. 616, 630 (1886).
[63] *See* Hanus & Relyea, *supra* note 60, at 562.
[64] *See, e.g.*, *The Computer and Invasion of Privacy: Hearings Before a Subcomm. of the H.R. Comm. on Gov't Operations,* 89th Cong. 195-213 (1966).
[65] 15 U.S.C. § 1681 (1970).

The Watergate scandal was the final straw, leading to the passage of the Privacy Act in late 1974, just four months after Richard Nixon's resignation in light of the scandal. The Act received wide bipartisan support while being promoted by new President Gerald Ford in his efforts to help America recover from the excesses of Watergate.[66] House and Senate debates on the legislation focused on horror stories of intrusions on a citizen's privacy and the threats that excessive surveillance might pose to freedom of speech and other constitutional rights.[67]

While the Privacy Act did not establish a right to privacy or a right to be left alone by the government, it did establish statutory protection for citizens who believe that the government is mishandling their personal information.[68] In other words, the Act places profound trust in the professionalism and discretion of government employees who have access to personal information. The Act established "fair information practices" for the collection and dissemination of information about individuals that is housed in federal agency files and databases.[69] The Act prohibits the disclosure of any such record without the written consent of the individual.[70]

The goal of the Privacy Act was to prevent the disclosure of personally identifiable records held by agencies, to grant individuals a right of access to documents in which they are identified, and to grant individuals the right to demand correction of documents about themselves that they believe to be inaccurate.[71] Such rules must be observed by "any Executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the [federal] Government

---

[66] *See* Hanus & Relyea, *supra* note 60, at 569-70.
[67] *See, e.g.*, H.R. REP. NO. 93-1416, at 4-6 (1974); S. REP. NO. 93-1183, at 11-12 (1974).
[68] *See* Hanus & Relyea, *supra* note 60, at 573.
[69] 5 U.S.C. § 552a(b) (2014).
[70] Id.
[71] *See Overview of the Privacy Act of 1974*, U.S. DEP'T OF JUST., https://www.justice.gov/opcl/policy-objectives [https://perma.cc/7M8F-CLBW].

(including the Executive Office of the President), or any independent regulatory agency."[72]

The Privacy Act also includes precise rules for how agency officials handle personal information that comes into their possession. "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[73] The Seventh Circuit has ruled that federal officials are "bound by the Privacy Act not to disclose any personal information and to take certain precautions to keep personal information confidential;"[74] while the Tenth Circuit has ruled that this applies to "not only the physical disclosure of the records, but also the accessing of private records" by any agency other than the one that originally possesses them.[75]

The Privacy Act includes exemptions, but these operate in the reverse fashion from FOIA's exemptions by compelling agencies to *not* withhold personal information in certain situations. There are twelve such exemptions, with most pertaining to fairly arcane agency procedures, but there are two that are relevant to this article's arguments. Exemption 7 of the Privacy Act compels agencies to disclose (typically to other agencies) documents that are needed for a law enforcement investigation,[76] and Exemption 8 works in a similar fashion if it is believed that other agencies could help preserve the person's health and safety.[77] Such requests from other agencies must be in writing,[78] and requests must not be based on "unsubstantiated

---

[72] 44 U.S.C. § 3502; *see also* 5 U.S.C. § 552a(a)(1) (2014).
[73] 5 U.S.C. § 552a(b) (2014).
[74] Big Ridge, Inc. v. Fed. Mine Safety & Health Review Comm'n, 715 F.3d 631, 650 (7th Cir. 2013).
[75] Wilkerson v. Shinseki, 606 F.3d 1256, 1268 (10th Cir. 2010).
[76] 5 U.S.C. § 552a(b)(7) (2014).
[77] 5 U.S.C. § 552a(b)(8) (2014).
[78] Doe v. DiGenova, 779 F.2d 74, 85 (D.C. Cir. 1985); Doe v. Naval Air Station, 768 F.2d 1229, 1232-33 (11th Cir. 1985).

allegations" in which the requesting agency exaggerates the need for law enforcement or safety intervention.[79]

It should be noted that the Privacy Act applies to actual "records" that are in an agency's possession,[80] and not necessarily to the content within, including information gained during surveillance. Therefore under the Act, the government can collect personal information on citizens however it pleases, even for exaggerated law enforcement or national security reasons, but must follow the Act's requirements for when and how to disclose the resulting documents. The Act does not attempt to reduce government record-keeping or even surveillance, and trusts agency employees as the protectors of private information that ends up in their possession. This was a change in government document-handling procedures that acknowledged that era's widespread public fear of abuses by unscrupulous officials.[81]

In the meantime, Congress had become concerned about the rising computerization of data collection practices.[82] Therefore the Privacy Act requires that the existence of governmental systems that collect personal information should not be concealed from the public.[83] As an indication of how much surveillance has been perpetuated without the public's knowledge since that provision was enacted in 1974, the American public did not know about many of the National Security Agency's (NSA) advanced internal surveillance mechanisms until the

---

[79] Schwarz v. Interpol, Office of Info. & Privacy, No. 94-4111, 1995 WL 94664, at *1 n.2 (10th Cir. Feb. 28, 1995).

[80] "Records" are defined as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4) (2014).

[81] *See* Hanus & Relyea, *supra* note 60, at 589.

[82] *See Overview of the Privacy Act of 1974*, *supra* note 71.

[83] This was a recommendation from an advisory committee whose research was cited in the House and Senate debates. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 41 (1973); s*ee also* H.R. REP. NO. 93-1416 (1974); S. REP. NO. 93-3418 (1974).

Snowden revelations of 2013.[84] As will be seen in the next section of this article, those systems were allowable under certain security-oriented statutes. However, under the Privacy Act the secrecy of their existence was illegal.[85]

Since Executive Branch agencies withhold so many documents from public view in order to protect the privacy of anyone named within, via either the Privacy Act or the privacy-oriented exemptions to FOIA, one might conclude that the American government cares deeply about the privacy of its citizens. Unfortunately, a look at the government's attitudes toward privacy in other policy areas shows that this concern is only being expressed to avoid disclosing documents–or more cynically, the government shows concern for privacy as an easy way to maintain its secrets. As has been seen with the rise of the "surveillance state" after 2001, the American government enjoys keeping secrets but expects the citizenry to do the opposite. More specifically, the Privacy Act was passed because Congress was becoming concerned about the rapidly expanding electronic surveillance of citizens. That trend was just barely getting started in 1974, and government use of electronic surveillance, with often exaggerated security and law enforcement justifications (which are forbidden by the Privacy Act when handling the resulting documents[86]), has become more and more intrusive and pervasive. That old Congressional concern about privacy has moved in the opposite direction since the Privacy Act was passed.

IV. Privacy Unexceptionalism in the Surveillance State

In the ongoing fight against terrorism and efforts to protect America from foreign enemies, the American government has displayed an attitude toward privacy that is essentially the opposite of that shown when it wishes to keep documents secret. Whereas Executive Branch agencies have made privacy dubiously *exceptional* when deciding to reject requests for documents, the cluster of agencies involved in the

---

[84] *See generally* GREENWALD, *supra* note 9.
[85] *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, *supra* note 82. No judicial discussion of this conundrum could be found during the research for this article.
[86] *See* 5 U.S.C. §§ 552a(b)(7)-(8) (2014).

national security effort have declared (though not in so many words) that personal privacy is so *unexceptional* that it rarely gets a fair hearing in debates about modern surveillance programs and techniques.

Since 2001, the drive to protect America from real and supposed enemies has caused the national security and law enforcement establishments to come together, with both using similar surveillance and data tracking techniques.[87] The leaders of this rising surveillance state have been wise in not publicly stating their disregard for personal privacy, and have in fact made public statements in which they claim to support a balance between privacy and security. For example, former NSA Chief Keith Alexander is on record as saying that the agency "has executed its national security responsibilities with equal and full respect for civil liberties and privacy."[88] An agency spokesman issued a statement in 2014 proclaiming that "NSA's authorities to collect signals intelligence data include procedures that protect the privacy of US persons. Such protections are built into and cut across the entire process."[89]

These were statements tailored for the press and the public. The national security establishment's true thoughts on citizens' privacy have only been revealed in occasional leaked and declassified documents. For example, a document created by the NSA in 2000 noted that the agency had been trying to "rethink and reapply" its procedures toward the Fourth Amendment and citizen privacy long before the September 11 attacks. The agency argued (internally) that

---

[87] *See* Trevor Aaronson, *Welcome to Law Enforcement's "Dark Side": Secret Evidence, Illegal Searches, and Dubious Traffic Stops*, INTERCEPT (Jan. 9, 2018, 9:57 AM), https://theintercept.com/2018/01/09/dark-side-fbi-dea-illegal-searches-secret-evidence/ [https://perma.cc/3JZK-JX5M].

[88] Joe Davidson, *NSA Director Tells Staff to Remain Focused*, WASH. POST (June 27, 2013), https://www.washingtonpost.com/politics/federal_government/nsa-director-tells-staff-to-remain-%20focused/2013/06/27/41252d74-df5c-11e2-b2d4-ea6d8f477a01_story.html [https://perma.cc/KGM6-K6BE].

[89] Spencer Ackerman & Martin Pengelly, *NSA Statement Does Not Deny "Spying" on Members of Congress*, GUARDIAN (Jan. 4, 2014, 3:31 PM), https://www.theguardian.com/world/2014/jan/04/nsa-spying-bernie-sanders-members-congress [https://perma.cc/T9JG-3FSD].

this new outlook was necessary to conduct the pervasive surveillance enabled by a "powerful, permanent presence on a global telecommunications network."[90] The NSA has further claimed that the complexity of surveillance technology allows infringements on privacy and other civil liberties unless someone argues otherwise.[91] The agency has also admitted to collecting "metadata" on citizens, but made the misleading statement that metadata is strictly impersonal and does not reveal personally-identifiable information.[92]

The official national security apparatus (made up of entities like the NSA, Central Intelligence Agency [CIA], Department of Homeland Security, and several others[93]) is required by law to uphold the civil rights and civil liberties of persons under investigation, and privacy is listed as one of the values to be upheld.[94] The Director of National Intelligence, who oversees the activities of the various agencies

---

[90] *See* NATIONAL SECURITY AGENCY & CENTRAL SECURITY SERVICE, TRANSITION 2001, at 32 (2000).

[91] Jay Hathaway, *NSA Broke Privacy Rules Because Its Phone Data System Was Too "Complex,"* DAILY DOT (Sept. 10, 2013, 2:48 PM), https://www.dailydot.com/debug/nsa-phone-data-privacy-violations-revealed/ [https://perma.cc/7NXY-2LV3]. This statement was originally made by then-Director of National Intelligence James Clapper in an internal agency blog post, which is no longer available online at the time of writing.

[92] *See* Spencer Ackerman, *NSA Review Panel Casts Doubt on Bulk Data Collection Claims*, GUARDIAN (Jan. 14, 2014, 4:44 PM), https://www.theguardian.com/world/2014/jan/14/nsa-review-panel-senate-phone-data-terrorism [https://perma.cc/MJ62-WVME]. The term *metadata* is most easily described with an illustration from an older communications technology–a letter mailed to a friend. The *content* of this letter is the actual message to the friend inside the envelope, while the *metadata* is the address and the post office's date/time stamp on the outside of the envelope. In modern electronic communications, *metadata* consists of IP addresses and routing numbers that may appear to be obtuse programming code, but it can be used quite easily to determine the identity of the persons who sent and received the transmission, and oftentimes a direct read of the *content* is not necessary. *See infra* notes 167-68 and accompanying discussion.

[93] The Director of National Intelligence oversees myriad federal agencies in national security and law enforcement. Office for Civil Rights and Civil Liberties, U.S. Dep't of Homeland Sec., *National Security Act*, JUST. INFO. SHARING, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1280 [https://perma.cc/KYA9-CHDT].

[94] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, § 1016(d)(2)(A), 118 Stat. 3638, 3666.

involved in the national security effort, must appoint a Civil Liberties Protection Officer to "ensure that protection of civil liberties and privacy is appropriately incorporated in the policies and procedures developed for and implemented by" those agencies.[95] It is important to note that the civil liberties being protected in these stipulations include those enjoyed not just by persons being investigated, but also by the general public, which has the right to inspect agency operations.[96]

Regardless, the national security establishment has used privacy concerns to justify keeping its own operations secret, though this privacy is typically enjoyed by agents, not the people they are investigating. For example, the Ninth Circuit has held that "FBI agents have a legitimate interest in keeping private matters that could conceivably subject them to annoyance or harassment."[97] Information about hiring practices at security agencies, and agents' interactions with consultants who recommend potential new agents, have also been ruled as sufficiently private to withhold from public disclosure.[98] This trend has reached some absurd heights in which privacy, but this time the privacy of government employees, trumped significant matters of the public interest.

For example, in a dispute over a FOIA request for documents from the Defense Intelligence Agency, a district court upheld that agency's decision to withhold documents about a suspected mass grave containing militants who had been killed during the conflict in Afghanistan, because some agency employees were named within and

---

[95] *Id*. at sec. 1011, § 103(b)(1), 118 Stat. 3638, 3658.

[96] *See, e.g*., Martin E. Halstuk & Eric B. Easton, *Of Secrets and Spies: Strengthening the Public's Right to Know About the CIA*, 17 STAN. L. & POL'Y REV. 353, 379 (2006).

[97] Lahr v. Nat'l Transp. Safety Bd., 569 F.3d 964, 977 (9th Cir. 2009) (concerning a rejected FOIA request for documents on the investigation of a plane crash); Hunt v. FBI, 972 F.2d 286, 288 (9th Cir. 1992) (concerning a rejected FOIA request for documents on an internal FBI investigation of an agent who had been accused of misconduct).

[98] Holland v. CIA, Civ. A. No. 92-1233, 1992 WL 233820 at *14-15 (D.D.C. 1992) (concerning the CIA's rejection of a FOIA request, on privacy grounds, for information on a civilian who had written letters of recommendation for some potential new agents).

disclosure could have jeopardized their privacy.[99] This reasoning was also used by the same district court to allow a plethora of agencies in the national security and law enforcement establishment—including the Federal Bureau of Investigation, Department of Justice, Drug Enforcement Agency, and Department of State—to withhold requested documents on their investigations into the person who requested those documents. That person was told that he was violating his own privacy by requesting documents that could help him understand government investigations of himself.[100]

Meanwhile, the NSA and others in the security and law enforcement establishment have performed some minor administrative rulemaking on agency privacy practices, in the expectation that disputes will arise when large numbers of innocent people are surveilled by public camera systems, drones, data mining, and the like. However, Christopher Slobogin considers this trend to be self-serving and that enforceable legislation to oversee such agency efforts is needed.[101] Those internal rulemaking efforts may or may not be in good faith, but the pattern of modern national security investigations shows that privacy has fallen far behind the other concerns of the agencies involved.

a. National Security Investigations

Political pressures, particularly after the terrorist attacks of September 11, 2001, have justified a significant expansion of the American national security establishment.[102] At the same time, new

---

[99] Physicians for Human Rights v. Dep't of Def., 778 F. Supp. 2d 28, 36 (D.D.C. 2011).

[100] Miller v. Dep't of Justice, 562 F. Supp. 2d 82, 112 (D.D.C. 2008). This ruling, and that in the *Physicians for Human Rights* case discussed in *supra* note 99, were predicated on FOIA Exemption 3, 5 U.S.C. § 552(b)(3) (2016), which allows the withholding of documents that have been declared off-limits in a different statute.

[101] *See* Slobogin, *supra* note 11, at 1764.

[102] The primary statute that expanded the national security establishment was the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), Pub. L. No. 107-56, 115

telecommunications technologies have facilitated the surveillance of the private communications of practically all American citizens, and the agencies have made full use of such technologies in the belief that enemies can be detected before they strike.[103] In fact, Professor Peter Swire has thanked personal communications technologies for ushering in the "golden age of surveillance."[104]

Modern electronic surveillance has complicated privacy protections in a distinct fashion. When telecommunications and Internet activity are surveilled at the system level, as is often the case at the NSA, not just individual privacy is at stake but group privacy as well. Modern surveillance practices, dubbed "panvasive" by Slobogin, "are not aimed at specific individuals, but rather involve government invasion of the privacy or autonomy of a number of people, despite foreknowledge that most if not all of them are innocent of any wrongdoing."[105] Searches of wide groups of people is typically performed without any sort of warrant, but nonetheless have been generally held as permissible under Fourth Amendment procedures due to the supposed public interest in protection from terrorism.[106]

Stat. 272 (2001). The USA PATRIOT Act will be discussed in more detail at *infra* notes 176-183 and accompanying text.

[103] The leading theoretician on this evolution of national security practices is Bruce Schneier, a network security expert and critic of the modern expansion of surveillance and the affiliated government policies. *See, e.g.*, BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD (2015); Bruce Schneier, *Security or Surveillance?*, LAWFARE (Feb. 1, 2016, 1:01 PM), https://www.lawfareblog.com/security-or-surveillance [https://perma.cc/Z5VZ-HS2Q].

[104] *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*, *Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 6–12 (2015) (testimony of Peter Swire, Huang Professor of Law and Ethics, Scheller College of Business, Georgia Institute of Technology).

[105] *See* Slobogin, *supra* note 11, at 1726.

[106] *Id.* at 1730. Slobogin located one ruling in which the Supreme Court called for a balancing test between security and privacy, but the ruling is considered to be an outlier because it was before the September 11 attacks: Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 619 (1989) ("When faced with such special needs [national security efforts], we have not hesitated to balance the governmental and privacy interests to assess the practicality of the warrant and probable-cause requirements in the particular context.").

However, none of this was an abrupt about-face in the aftermath of the September 11 attacks, and was instead an enhancement of surveillance practices that had been just as secretive, if less technologically advanced, for years previously. Long before the September 11 attacks, Executive Branch agencies in the security realm, most notably the NSA and CIA, had been secretive about their operations and typically resisted FOIA requests for information via Exemption 1,[107] which allows the withholding of national security-related information. The agencies typically used this strategy without seeing any need to prove that the requested documents were truly relevant to national security, and this behavior was almost always condoned by the courts.[108] This longtime strategy went into overdrive after the September 11 attacks, and has been extensively analyzed elsewhere.[109] The national security establishment also enjoys the protection of several statutes, such as the National Security Act of 1947[110] and the Central Intelligence Agency

---

[107] 5 U.S.C. § 552(b)(1) (2016) (allowing withholding of documents that "(A) [are] specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order").

[108] *See, e.g.*, Danae J. Aitchison, *Reining in the Glomar Response: Reducing CIA Abuse of the Freedom of Information Act*, 27 U.C. DAVIS L. REV. 219 (1993); Robert P. Deyling, *Judicial Deference and De Novo Review in Litigation Over National Security Information Under the Freedom of Information Act*, 37 VILL. L. REV. 67 (1992); Scott A. Faust, *National Security Information Disclosure Under the FOIA: The Need for Effective Judicial Enforcement*, 25 B.C. L. REV. 611 (1983); Jonathan Turley, *Through a Looking Glass Darkly: National Security and Statutory Interpretation*, 53 S.M.U. L. REV. 205 (2000).

[109] *See, e.g.*, Martin E. Halstuk, *Holding the Spymasters Accountable after 9/11: A Proposed Model for CIA Disclosure Requirements Under the Freedom of Information Act*, 27 HASTINGS COMM. & ENT. L.J. 79 (2004); Halstuk & Easton, *supra* note 96; David B. McGinty, *The Statutory and Executive Development of the National Security Exemption to Disclosure Under the Freedom of Information Act: Past and Future*, 32 N.KY. L. REV. 67 (2005); Kathleen A. McKee, *Remarks on the Freedom of Information Act: The National Security Exemption in a Post 9/11 Era*, 4 REGENT J. INT'L L. 263 (2006); Susan Nevelow Mart & Tom Ginsburg, *Dis-]informing the People's Discretion: Judicial Deference Under the National Security Exemption of the Freedom of Information Act*, 66 ADMIN. L. REV. 725 (2014).

[110] 50 U.S.C. §§ 3001-234 (2004).

Act of 1949,[111] that expressly allow most, if not all, investigatory documents to remain off-limits to the public.[112]

The national security establishment has also been known to cite the FOIA privacy exemptions when refusing requests for documents. This is where the agencies' inconsistent attitudes toward privacy take on politicized overtones depending on the needs of the surveillance state, and regardless of the public interest. In a dispute directly related to the September 11 attacks, *Center for National Security Studies v. U.S. Department of Justice*, a coalition of public interest groups filed a FOIA request with the Justice Department for the names of persons who had been detained during the investigation of the attacks, plus their dates of arrest and reasons for detention or release. That investigation had swept up more than one thousand people.[113] The agency withheld most of the requested information; surprisingly, it did not cite FOIA Exemption 1 (national security),[114] but it did cite three

---

[111] 50 U.S.C. §§ 3501-24 (1993).

[112] *See* Benjamin W. Cramer, *Old Love for New Snoops: How Exemption 3 of the Freedom of Information Act Enables an Irrebuttable Presumption of Surveillance Secrecy*, 23 COMM. L. & POL'Y 91, 113-19 (2018). Exemption 3 of FOIA, 5 U.S.C. § 552(b)(3) (2016), allows the withholding of documents that are "specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld." In other words, this exemption allows the withholding of documents that have already been declared non-disclosable by a different statute. Exemption 3 is often utilized by the security-oriented agencies because their governing statutes, such as the National Security Act of 1947, declare many (if not all) documents in their possession to be off-limits. *See generally id*.

[113] 331 F.3d 918, 920-21 (D.C. Cir. 2003).

[114] Even though the agency did not directly cite Exemption 1, dissenting Judge David S. Tatel opined that an agency denial under that exemption would have been more believable than the law enforcement-related exemptions that were actually cited, due to the present urgency surrounding national security and the deference that had been offered to security agencies in the past thanks to that exemption's rules. *Id*. at 939.

law enforcement-related provisions under Exemptions 7(A), 7(C), and 7(F).[115]

The second of those, protecting the privacy of persons named in law enforcement documents, is most relevant to the present discussion. The Justice Department declared that the detainees have "an obvious privacy interest cognizable under Exemption 7(C) in keeping secret the fact that they were subjects of a law enforcement investigation."[116] The Circuit Court for the District of Columbia agreed with this reasoning and affirmed the withholding of the requested documents.[117] The court also declared that "investigatory information" can be withheld under FOIA because it does not shed light on the "government adjudicative process,"[118] thus echoing the problematic "central purpose" test from the *Reporters Committee* precedent.[119]

The majority ruling in the *Center for National Security Studies* case, in favor of withholding the requested documents, has served as a precedent in which courts have generally given deference to security agency concerns about supposed damage to personal privacy that could come from disclosure, with few if any entreaties to agencies to actually describe those potential harms in detail.[120] Furthermore, the

---

[115] 5 U.S.C. §§ 552(b)(7)(A), 552(b)(7)(C), 552(b)(7)(F) (2002). Exemption 7(C) is discussed regularly throughout in this article; for the full text see *supra* note 3. Exemption 7(A) allows the withholding of law enforcement-related records that "could reasonably be expected to interfere with enforcement proceedings;" Exemption 7(F) allows the withholding of law enforcement-related records that "could reasonably be expected to endanger the life or physical safety of any individual."

[116] 331 F.3d at 945.

[117] *Id*. at 937.

[118] *Id*. at 936.

[119] *See supra* notes 21-28 and the accompanying discussion.

[120] *See e.g*., L.A. Times Commc'ns, LLC v. Dep't of Army, 442 F. Supp. 2d 880, 899-900 (C.D. Cal.; 2006) (a dispute over a FOIA denial in which the newspaper requested documents detailing "serious incident reports" submitted by private contractors during wartime operations in Iraq; the request was denied by the Army under various provisions of the law enforcement exemptions); Scudder v. CIA, 25 F. Supp. 3d 19, 40, n.11 (D.D.C. 2014) (regarding a rejected FOIA request for internal CIA documents); Larson v. Dep't of State, 565 F.3d 857, 864-865 (D.C. Cir. 2009) (involving a rejected FOIA request to the NSA, CIA, and Department

District Court for the District of Columbia and its district courts have continued to differentiate, as did the majority in the *Center for National Security Studies* case, between "investigatory information" that can be withheld under FOIA and material that can be disclosed because it does not shed light on a "government adjudicative process."[121] This further repeats the difficulties created by the *Reporters Committee* precedent, as the requester must argue that the requested document sheds some sort of light on governmental operations before being allowed to see that same document, and simply because a person's name is listed in whatever fashion.

In a lengthy dissent to the *Center for National Security Studies* ruling, which is considerably longer than the majority ruling, Judge David S. Tatel eviscerated the government's professed concerns about personal privacy, uncovering some of the contradictions at the heart of this article's arguments.[122] Judge Tatel found the Department of Justice's primary rationale to be unconvincing because the government, perhaps succumbing to public demands for action, had already released the names of several suspects including Abdulla Al Muhajir, Issaya Nombo, and Mohammad Mansur Jabarah with no particular regard for their personal privacy, and had also released the names of many of the attorneys representing detainees.[123] Judge Tatel opined further that even though there would be a stigma when one's name is attached to a criminal investigation, much less the investigation of a major disaster like the September 11 attacks, that person's privacy interest "is clearly outweighed by the public interest in knowing whether the government, in investigating those heinous crimes, is violating the rights of persons it has detained."[124]

---

of State for documents related to American operations in Guatemala in the 1970s-80s).

[121] *See, e.g.*, Dhiab v. Trump, 852 F.3d 1087, 1104 (D.C. Cir. 2017) (involving a rejected FOIA request for videos believed to document the torture of detainees at Guantanamo Bay detention camp); *In re* Guantanamo Bay Detainee Cases, 355 F. Supp. 2d 443 (D.D.C. 2005).

[122] 331 F.3d at 937 (Tatel, J., dissenting).

[123] Id. at 945, 950-51.

[124] *Id*. at 945-46. This conclusion was supported by the Circuit Court precedents Nation Magazine, Wash. Bur. v. U.S. Customs Svc., 71 F.3d 885, 894 (D.C. Cir.

Judge Tatel was also convinced, thanks to recent news reports, that the federal government was abusing the investigative process by detaining suspects without charge or access to counsel, and that this offered "compelling" evidence that the requested documents were in the public interest because they could shed light on agency wrongdoing.[125] In conclusion, Judge Tatel pronounced the agency's claims on the need to protect privacy in this FOIA denial to be "profoundly wrong," and that it unfairly shifted the burden of proof from the agency to the requesters.[126] Here Judge Tatel acknowledged, at least indirectly, the weaknesses of the *Reporters Committee* precedent.

In his concluding remarks, Judge Tatel noted that persons under investigation may indeed have personal privacy rights, but the government's claims of respecting that privacy did not match its actions during the September 11 investigations.[127] This was only a dissenting opinion in the instant case, and judges in future cases have shown little awareness of Judge Tatel's concerns, which would largely disappear from discussions of surveillance overreach in the following decade.

Judge Tatel's dissent in the *Center for National Security Studies* case was acknowledged by the District of Columbia District Court in 2006 in a statement on how categorical withholding of security documents by government agencies without further discussion "would eviscerate the principles of openness in government that the FOIA embodies."[128]

1995), and Am. Fed'n of Gov't Employees, AFL-CIO v. Dep't of Housing & Urban Dev., 118 F.3d 786, 794 (D.C. Cir. 1997).

[125] 331 F.3d at 946-48. Here Judge Tatel cited precedent in Rosenfeld v. Dep't of Justice, 57 F.3d 803, 812 (9th Cir.1995), in which the Ninth Circuit ruled that FOIA Exemption 7(C) does not justify withholding the identities of persons being investigated (by the FBI in that case) if the documents in question could shed light on the agency's investigative practices.

[126] 331 F.3d at 950.

[127] *Id*. at 951-52.

[128] Long v. U.S. Dep't of Justice, 450 F. Supp. 2d 42, 76 (D.D.C. 2006) (concerning a FOIA request for documents on the management of a database that collects documents on United States Attorneys; the agency was ordered to release some documents while the remainder of its FOIA denial was upheld).

This was not dispositive to the FOIA dispute at hand, however, because the court concluded that documents could be withheld as long as government agencies provide legitimate concerns of risks to security investigations if requested documents are disclosed, and that courts should defer to such concerns.[129] Notwithstanding this ruling, which did not lead to disclosure anyway, the judges in later disputes over the disclosure of information on surveillance and security investigations have barely noticed the national security establishment's functionally absurd use of privacy values to justify the secrecy of those operations.

b. Reasonable Expectation of Privacy

The national security establishment has found yet another way to justify its curtailment of personal privacy, by assuming that Americans may not be justified in expecting to have privacy at all. As opposed to the government's concern for personal privacy when withholding agency documents, the NSA and its brethren have long taken advantage of Supreme Court precedents confirming that citizens actually have no "reasonable expectation of privacy" toward electronic communications, which of course are the focus of the modern surveillance state.

As far back as the *Olmstead* case in 1928, the Supreme Court ruled that there is no violation of rights, under the Fourth or Fifth Amendments, when law enforcement personnel wiretap personal telephone lines.[130] Wiretapping laws dating back to the early Twentieth Century, and their attendant judicial precedents, are still used to justify modern electronic surveillance of telecommunications and Internet usage.[131] The *Olmstead* decision was partially overturned in the 1967 *Katz* ruling, if wiretapping is done in a public place.[132] That ruling was based on a new conception of *reasonable expectation*

---

[129] *Id*. at 77-78.
[130] Olmstead v. U.S., 277 U.S. 438 (1928).
[131] *See* Blake Covington Norvell, *The Constitution and the NSA Warrantless Wiretapping Program: A Fourth Amendment Violation*, 11 YALE J. L. & TECH. 228, 235-43 (2008); Cramer, *supra* note 112, at 121-22.
[132] Katz v. U.S., 389 U.S. 347 (1967).

of privacy which citizens apparently enjoy in public,[133] though later courts have ruled that this expectation is sacrificed when people use telecommunications services voluntarily, or when there is a public interest in security and law enforcement inspection of those same services.[134]

The *reasonable expectation of privacy* becomes distorted when someone other than the government (police, security officials, etc.) has access to personal data. When private companies like telecommunications firms, and now Internet firms, have access to personal data, the assumption is that the person has handed this information over voluntarily, at which point the reasonable expectation of privacy expires even if that information is later forwarded to the government. This is known as the *third-party effect*,[135] which was first addressed by the Supreme Court in *Smith v. Maryland* in 1979,[136] resulting in a landmark ruling that the American national security establishment has used to justify its activities ever since. In short, individuals can be blamed for sacrificing their own privacy by handing data to telecommunications companies that then hand it to the government, and in this realm the government is far less concerned about personal privacy than it is when denying FOIA requests for documents about its operations.

The *Smith* case involved a criminal defendant who had been suspected of making harassing phone calls to his victim. The police inspected Mr. Smith's calling records and determined that he had indeed called the victim's phone number, leading to his arrest. Mr. Smith argued that the police's inspection of phone company records of his calls was a search of his personal effects, and per the Fourth Amendment a warrant should have been obtained. The Supreme Court ruled that

---

[133] The phrase *reasonable expectation of privacy*, which has since been used in many (if not most) judicial decisions on electronic surveillance, was first used by Justice John Marshall Harlan in a concurrence to the *Katz* ruling. *Id*. at 361; s*ee also* Slobogin, *supra* note 11, at 1746.
[134] *See* Yesner, *supra* note 11, at 160.
[135] *See* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 102-10 (2011).
[136] 442 U.S. 735.

Smith "voluntarily conveyed numerical information to the telephone company."[137] Furthermore, as a phone company customer, Smith should have known that the company would need to know this information in order to function properly as it connected his calls. Thus, he did not have a reason to expect his calling information to be private.[138]

Furthermore, in *Smith* the Court acknowledged the *third-party effect*, but in favor of telecommunications network companies, by ruling that warrant procedures under the Fourth Amendment apply when government authorities search you and your possessions directly, but *not* when they search information that you have given to a third party (such as a phone company) voluntarily.[139] This ruling established the precedent that a person's use of a telecommunications network is completely voluntary, which may have been a viable conclusion for old landline telephone systems in 1979, but which may no longer be tenable in modern times when advanced electronic networks are heavily integrated into everyday life, while those networks collect massive amounts of personal data that is of great interest to the surveillance state.[140]

Thanks to *Smith v. Maryland*, the "reasonable expectation of privacy" question, and the fact that Americans do not have this expectation, has justified government searches of the information collected by far more advanced telecommunications and Internet systems. For example, in 1983 the Supreme Court ruled that individuals do not have a reasonable expectation of privacy on public thoroughfares that are surveilled by police cameras,[141] and three years later the Court ruled that aerial surveillance of public places is not a violation of Constitutional rights.[142]

---

[137] *Id*. at 744.
[138] *Id*. at 743.
[139] *Id*. at 744.
[140] Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 L. & PHIL. 559 (1998).
[141] U.S. v. Knotts, 460 U.S. 276, 281-82 (1983) (using the synonymous term "legitimate expectation of privacy").
[142] California v. Ciraolo, 476 U.S. 207, 213-15 (1986).

Smith v. Maryland and its followers have been used to justify ultra-modern surveillance of citizens via drones, GPS, and data mining.[143] While the Supreme Court stated in 2001 that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology,"[144] the law enforcement and national security apparatus has been allowed to reap the benefits of these new technologies, as long as proper procedures are observed. For example, in 2012 the Court stated in the *Jones* case that direct surveillance of a criminal suspect's movements via GPS is a "search" under the Fourth Amendment, but ultimately ruled that the police officers in the case had followed warrant procedures properly.[145] The Court merely hinted, with evident reluctance, that privacy issues may arise when the resulting data is collected long-term[146] and/or disseminated over telecommunications networks,[147] where the citizen's lack of a reasonable expectation of privacy from *Smith v. Maryland* still holds.

Two years later, the Supreme Court reached a similar determination on how there is no privacy violation if warrant procedures are followed properly when police examine a person's cellular phone.[148] The Court has since added some narrow categories of information for which proper warrant procedures must be followed before government agents can collect the data, including location information housed in one's "smart" phone.[149] In that ruling the Court determined that a citizen has a reasonable expectation of privacy concerning his whereabouts and physical movements over time as recorded by modern

---

[143] *See* Slobogin, *supra* note 11, at 1746-47.
[144] Kyllo v. U.S., 533 U.S. 27, 33-34 (2001).
[145] U.S. v. Jones, 565 U.S. 400 (2012).
[146] *Id*. at 431 (Alito, J., concurring).
[147] *Id*. at 416 (Sotomayor, J., concurring).
[148] Riley v. California, 573 U.S. 373 (2014). Meanwhile, the Eleventh Circuit made a similar determination about proper warrant procedures when police examine cellular network calling records. U.S. v. Davis, 785 F.3d 498 (2015); the Supreme Court denied certiorari for this case in Davis v. U.S., 136 S. Ct. 479, 480 (2015).
[149] Carpenter v. U.S., 138 S. Ct. 2206 (2018).

telecommunications networks and devices,[150] but again it is important to note that this expectation can still be defeated when balanced with the needs of law enforcement, so long as agents follow the proper warrant procedures under the Fourth Amendment.[151]

It has thus been established in these precedents that citizens may have a reasonable expectation of privacy for personal information that can be found on modern telecommunications networks and the Internet, but even if they do, law enforcement officials can still obtain a warrant to see that information. The outcome for personal privacy is even less favorable when the national security establishment wants a person's communications records, especially if the fight against terrorism is used as justification. The power of antiterrorism rhetoric in defeating privacy concerns can be seen in a crucial split precedent at the district court level.

In two nearly identical cases directly inspired by the Snowden revelations, citizens sought damages from unauthorized surveillance by the NSA.[152] In late 2013, the federal district court in the District of Columbia ruled in *Klayman v. Obama* that the NSA's mass surveillance program is likely unconstitutional because modern telecommunications networks are pervasive, as is the ability of the government to track our usage of them, and this is a new phenomenon that deserves an updated Fourth Amendment analysis.[153] Here the District Court for the District of Columbia largely repudiated the *Smith v. Maryland* precedent on voluntary use of telecommunications networks, but this judgment has not been picked up by other courts in

---

[150] *Id*. at 2217.

[151] The Court ruled that the police officers in the instant case, who did not obtain a warrant before collecting cellular network information on Carpenter's locations and movements while he was under investigation, had violated his "reasonable expectation of privacy" in that type of information. But ultimately, the Court ruled that this violation could have been avoided with proper warrant procedures. *Id*. at 2221.

[152] Benjamin W. Cramer, *A Proposal to Adopt Data Discrimination Rather than Privacy as the Justification for Rolling Back Data Surveillance*, 8 J. INFO. POL'Y 5, 11-12 (2018).

[153] Klayman v. Obama, 957 F. Supp. 2d 1, 42 (D.D.C. 2013).

the face of antiterrorism rhetoric from the national security establishment.[154]

Just days after the *Klayman* ruling, the Southern District Court of New York ruled in *American Civil Liberties Union v. Clapper* that the NSA surveillance program did *not* violate the Fourth Amendment due to the reasonableness of national security investigations.[155] This ruling shows the power of the antiterrorism argument, which was discussed prominently in the ruling, while the citizen's reasonable expectation of privacy and the pervasiveness of modern data collection networks were not discussed at all.[156] These two rulings, which both addressed the NSA's attitude toward personal privacy when widely surveilling citizens to supposedly protect America from terrorist attacks, resulted in a split precedent that should be addressed by a higher court,[157] but this has not yet happened at the time of writing.

c. New Technologies and Emergency Surveillance

As far back as 1975, a Congressional committee opined that each Presidential administration develops its own new secrecy techniques that become more sophisticated over time, while also finding new ways to infringe on the privacy of citizens.[158] The government surveillance operations revealed by Edward Snowden in 2013 are a particularly insidious manifestation of this trend.[159] America has had great difficulty addressing the conflict between surveillance and privacy, and surveillance is currently winning this battle thanks to new technologies that enable mass tracking of individuals and a legal trend

---

[154] Cramer, *supra* note 152, at 9-10.
[155] American Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 756-57 (S.D.N.Y. 2013).
[156] Acknowledgement of these matters cannot be found in the *Clapper* ruling. *Id*.
[157] Gary Schmitt, *A Tale of Two Judges: The NSA on Trial*, WEEKLY STANDARD (Jan. 13, 2014, 12:00 AM), https://www.weeklystandard.com/gary-schmitt/a-tale-of-two-judges [https://perma.cc/MM3E-727H].
[158] Mart & Ginsburg, *supra* note 109, at 763, n.206.
[159] *Id*. at 763.

toward greater government access to personal information that is stored in modern telecommunications networks.[160]

The American government played a major role in developing the technologies that enabled the modern surveillance state, from punch cards to GPS, exhibiting a long-term goal of collecting data on citizens rather than observing any privacy rights they may have. Meanwhile, expanded government services in the second half of the Twentieth Century, such as welfare and unemployment benefits, required the collection of vast amounts of personal data for which the government developed the necessary databases and collection techniques. Those have since been adopted by the national security and law enforcement establishments.[161] The *Smith v. Maryland* precedent has enabled government surveillance of citizens through the use of the invasive techniques that it had a hand in inventing, because they are now used by telecommunications companies as well. Thus, we have seen the rise of a new "surveillance state" or "surveillance society" in which government collection of personal data is built into everyday technological reality, and this raises significant risks of privacy violations by government officials who find doing so to be easier and easier.[162]

A 2013 audit of operations at the NSA found thousands of privacy violations in just one year, averaging about eight per day. Furthermore, this only included unlawful invasions of the privacy of persons who were actually being investigated, and not the bystanders who were swept up in the mass electronic surveillance of large groups.[163] In the resulting report, an agency official was quoted as saying, "there was

---

[160] *See* Reidenberg, *supra* note 11, at 595.
[161] *See* Balkin, *supra* note 11, at 6.
[162] *See* Ohm, *supra* note 11, at 1318.
[163] *See* Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year Audit Finds*, WASH. POST (Aug. 15, 2013), https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html [https://perma.cc/97KF-NWPW]. The audit covered the period from April 2011 to March 2012 and was performed by inspecting documents that had been leaked by Edward Snowden.

nobody at [the] NSA who really had a full understanding of how the program was operating at the time."[164] The NSA and its affiliated agencies have a vast number of surveillance systems and techniques that even they do not completely understand, and it is unrealistic to assume that the other branches of the government can oversee them all continuously. This problem is exacerbated by the fact that only select members of Congress or the President's office are allowed to know about sensitive security programs.[165]

In the wake of the Edward Snowden revelations, the NSA and its brethren claimed that the *content* of personal communications was not being tracked, just the *metadata* attached to transmissions, perhaps to give the impression that metadata is not inherently invasive of one's personal privacy and therefore the agencies are dedicated to preserving that virtue. In this light, President Barack Obama stated that the collection of metadata by the national security apparatus is only "a minor infringement of privacy."[166] However, experts determined long ago that "NSA analysts can exploit [metadata] to develop a portrait of an individual, one that is perhaps more complete and predictive of behavior than could be obtained by listening to phone conversations or reading emails."[167]

At the higher level, after the September 11 attacks it did not take long for the American government to summarily dismiss most concerns about citizens' privacy if it could cite security and the fight against terrorism as justifications. In 2004, former Clinton Administration Secretary of Defense William S. Cohen, in his testimony to the 9/11 Commission, declared that it was important to develop a "meaningful,

---

[164] *See* Scott Shane, *Court Upbraided N.S.A. on Its Use of Call-Log Data*, N.Y. TIMES (Sept. 10, 2013), https://www.nytimes.com/2013/09/11/us/court-upbraided-nsa-on-its-use-of-call-log-data.html [https://perma.cc/6BY4-94U2].
[165] *See* Balkin, *supra* note 11, at 21.
[166] *See* Yesner, *supra* note 11, at 149. For an explanation of the term *metadata*, see *supra* note 92.
[167] *See* James Risen & Laura Poitras, *N.S.A. Examines Social Networks of U.S. Citizens*, N.Y. TIMES (Sept. 28, 2013), https://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html [https://perma.cc/DN7T-MGRB].

in-depth public discussion-among our citizens and not just our elected officials-regarding what *compromises on privacy* we are willing to accept in order to remain safe and free."[168] Overall, the 9/11 Commission stressed the need for knowledge amongst the citizenry about national security efforts, but expected the public to sacrifice privacy in return for protection and security from the government.[169]

The citizenry had also been told to accept greater governmental secrecy for these reasons. In a memo to Executive Branch agencies written just after the September 11 attacks, then- Attorney General John Ashcroft urged the agencies to disclose information "only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of information."[170] This appears to place privacy on par with other important values, but later in the same document, agencies are instructed to defend withholding decisions "unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records."[171] In other words, the ability of other agencies to perform investigations with the first agency's documents was paramount. This was not a new law making agency records more secretive, but it was an interpretation of FOIA procedures recommending that agencies find reasons to keep documents secret and to defend those decisions as justified by the fight against terrorism.[172] In practice, Ashcroft instructed agencies to only grant FOIA requests for documents after finding a "sound legal basis" for doing so, regardless of questions of privacy or the other values mentioned briefly at the beginning of the document.[173]

---

[168] *See Eighth Public Hearing Before the Nat'l Comm'n on Terrorist Attacks*, 108th Cong. 24 (2004), (statement of William S. Cohen, Sec. of Def.), http://govinfo.library.unt.edu/911/hearings/hearing8/cohen_statement.pdf (emphasis added).
[169] *See* Halstuk & Easton, *supra* note 96, at 383.
[170] *See* ATT'Y GEN. JOHN ASHCROFT, U.S. DEP'T JUSTICE, MEMORANDUM FOR HEADS OF ALL FEDERAL DEPARTMENTS AND AGENCIES (2001), https://www.justice.gov/archive/oip/011012.htm.
[171] *Id*.
[172] *See* McGinty, *supra* note 109, at 113.
[173] *See* Keith Anderson, *Is There Still a "Sound Legal Basis?": The Freedom of Information Act in the Post-9/11 World*, 64 OHIO ST. L.J. 1605 (2003); Jane E.

Paradoxically, on that same day Ashcroft instructed federal agencies to balance the need for an "informed citizenry" with the public interest in "safeguarding our national security, enhancing the effectiveness of our law enforcement agencies, protecting sensitive business information and, not least, preserving personal privacy."[174] Here, Ashcroft again appeared to be respecting privacy as a value equal to the others, but there is little evidence that this supposed concern came to fruition as agencies were instructed to keep citizens from knowing how their privacy was being violated by the rising surveillance state. Once again, this could be justified with the need for security. The new laws coming together at the time, such as the USA PATRIOT Act,[175] placed a much sounder legal basis on the fight against terrorism, with significantly less regard for other values including privacy.[176]

National emergencies demonstrate that values such as privacy and public knowledge can be redefined and restricted to reflect the state of public fear, while courts are likely to sympathize with an emergency curtailment of civil rights.[177] For example, the USA PATRIOT Act, which according to well-placed critics included severe curtailments of privacy,[178] was rushed through Congress during a period of national

---

Kirtley, *Transparency and Accountability in a Time of Terror: The Bush Administration's Assault on Freedom of Information*, 11 COMM. L. & POL'Y 479, 491 (2006).

[174] *See* ASHCROFT, *supra* note 170.

[175] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001).

[176] *See* Kathleen A. McKee, *Remarks on the Freedom of Information Act: The National Security Exemption in a Post 9/11 Era*, 4 REGENT J. INTL' L. 263, 272-73 (2006).

[177] *See* Wagner, *supra* note 40, at 396.

[178] *See* ANDREW P. NAPOLITANO, THE CONSTITUTION IN EXILE: HOW THE FEDERAL GOVERNMENT HAS SEIZED POWER BY REWRITING THE SUPREME LAW OF THE LAND 209-237 (2006); RON PAUL, THE REVOLUTION: A MANIFESTO 110 (2008). Andrew Napolitano, a former state Superior Court judge, also wrote that "The PATRIOT Act and its progeny are the most abominable, unconstitutional governmental assaults on personal freedom since the Alien and Sedition Acts of 1798." *See* ANDREW P. NAPOLITANO, THE FREEDOM ANSWER BOOK: HOW THE GOVERNMENT IS TAKING AWAY YOUR CONSTITUTIONAL FREEDOMS 129 (2012).

anxiousness just after the September 11 attacks and was passed into law before most of the representatives had read its text.[179] The USA PATRIOT Act obliterated many previously-enacted checks on the federal government's ability to obtain personal information about citizens and track their movements.[180] The Act also enabled the trading of citizens' personal information among a multitude of secrecy-prone agencies in the national security apparatus,[181] and weakened pre-existing privacy laws like the Fair Credit Reporting Act and Financial Right to Privacy Act if mandated by a security investigation.[182]

Hence, the public has been expected to give up privacy protections for reasons of security, which is easy to justify during times of real or supposed emergency.[183] Benjamin Franklin's famous quote, "[t]hose who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety,"[184] has held true after the September 11 attacks, but the American government has crafted rules to force this choice on the citizenry by disregarding privacy by fiat, and this strategy has largely been endorsed by the courts.

Judicial deference for surveillance when justified by security has only experienced one notable roadblock since the earliest days of wiretapping. In a concurrence to the *Katz* ruling in 1967, Supreme Court Justice William O. Douglas declared that such deference would create a "wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels 'national security' matters," particularly

---

[179] *See* Yesner, *supra* note 11, at 173-74.
[180] *See* Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy Under the USA Patriot Act*, 80 DENV. U. L. REV. 375, 378 (2002).
[181] USA PATRIOT Act § 504.
[182] *See* Mell, *supra* note 180, at 393-94.
[183] *See* Cramer, *supra* note 154, at 6-12.
[184] SUZY PLATT, ED. RESPECTFULLY QUOTED: A DICTIONARY OF QUOTATIONS 201 (1992). This quote is often used by privacy activists and critics of surveillance, but when taken in context, Franklin was talking about international financial transactions. *See* Eugene Volokh, *Liberty, Safety, and Benjamin Franklin*, WASH. POST (Nov. 11, 2014, 1:18 PM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/11/liberty-safety-and-benjamin-franklin/?noredirect=on&utm_term=.b02307ce6859 [https://perma.cc/BC6L-PFPK].

because it was unreasonable to assume that Executive Branch officials could be "neutral and disinterested" observers of the unintended consequences of national security efforts.[185]

But otherwise, the modern surveillance state has faced little resistance from the courts. Legal scholar David Cole has declared that "courts are largely ineffectual on matters of national security" after reviewing ignoble historical episodes like President Abraham Lincoln's suspension of *habeas corpus* during the Civil War, the internment of Japanese Americans during World War II, and Senator Joseph McCarthy's harassment of citizens that were merely suspected of Communist sympathies during the Red Scare of the 1950s.[186] All of these received deference from the Supreme Court.[187] The government's overuse of security concerns to justify increased secrecy and invasions of personal privacy could be legitimate, or it could be mere opportunism in light of public outrage over a security emergency, at which time legislators and the judiciary willingly allow rights to be curtailed.[188]

America is very slowly recovering from the security-obsessed curtailment of civil liberties after the September 11 attacks. Many of the USA PATRIOT Act's surveillance-enabling provisions sunsetted in 2015, though some were preserved in the USA FREEDOM Act of that year and remain in effect.[189] Some of the more egregious NSA surveillance programs were discontinued in 2017 due to conflicts with other statutes,[190] and another program that tracks phone calls was

---

[185] Katz v. U.S., 389 U.S. at 359-60 (Douglas, J., concurring).
[186] David Cole, *The Priority of Morality: The Emergency Constitution's Blind Spot*, 113 YALE L.J. 1753, 1761 (2004).
[187] *See id*.
[188] *See* Wagner, *supra* note 40, at 415. Wagner detected this process during the War on Drugs.
[189] Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act (USA FREEDOM Act), Pub. L. No. 114-23, 129 Stat. 268 (2015).
[190] Andy Greenberg, *A Big Change in NSA Spying Marks a Win for American Privacy*, WIRED (Apr. 28, 2017, 5:45 PM), https://www.wired.com/2017/04/big-change-nsa-spying-marks-win-american-privacy/ [http://perma.cc/9HZL-DB26].

reportedly shut down in early 2019.[191] However, many of the statutory provisions that allow these types of surveillance remain on the books at the time of writing, and the absence of direct legal authorization has not stopped the NSA and its brethren from taking advantage of the technological ease of surveillance systems that already exist.[192]

Despite the references to privacy in the orders and statutes used by the national security establishment, legal scholar Paul Ohm has declared that privacy is disappearing in the modern world, thanks to both new technologies and increased governmental surveillance.[193] Even when they claim to observe privacy protections, national security and law enforcement agencies can get away with not doing so thanks to old precedents on the *reasonable expectation of privacy* and *third-party effect* doctrines from Fourth Amendment jurisprudence,[194] with little concern for the fact that those precedents pertained to old-school law enforcement by police officers on foot rather than new-school surveillance by mysterious agents sitting at computer terminals.[195] Since existing Fourth Amendment jurisprudence has determined that the Amendment does not confer a comprehensive right of privacy, it has been largely unable to restrain modern electronic surveillance.[196] When that surveillance is framed as a matter of national security and

---

[191] Charlie Savage, *Disputed N.S.A. Phone Program Is Shut Down, Aide Says*, N.Y. TIMES (Mar. 4, 2019), https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html [https://perma.cc/9HZC-TRAE].

[192] *See* Jason M. Breslow, *With or Without the Patriot Act, Here's How the NSA Can Still Spy on Americans*, FRONTLINE (June 1, 2015), https://www.pbs.org/wgbh/frontline/article/with-or-without-the-patriot-act-heres-how-the-nsa-can-still-spy-on-americans/ [https://perma.cc/492U-L62U].

[193] *See* Ohm, *supra* note 11, at 1334-36.

[194] *See supra* notes 130-139 and accompanying discussion.

[195] *See* Ohm, *supra* note 11, at 1335; SOLOVE, *supra* note 135, at 114-15.

[196] *See* Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After Lawrence*, 57 UCLA L. REV. 1, 56 (2009); Conor Friedersdorf, *The NSA Wants America's Most Powerful Corporations to Be Dependent on It*, ATLANTIC (July 16, 2013), https://www.theatlantic.com/politics/archive/2013/07/the-nsa-wants-americas-most-powerful-corporations-to-be-dependent-on-it/277822/ [https://perma.cc/4EAL-GF98].

antiterrorism, the courts have not hesitated in favoring surveillance over privacy.[197]

Therefore, the surveillance state's claims of protecting personal privacy as a virtue are not supported by its actions in conducting national security-oriented investigations, and few courts have noticed that the agencies' concerns for privacy are disingenuous. This arm of the American government, through its actions if not necessarily its words, has engaged in a new form of *privacy unexceptionalism* by largely disdaining privacy as an issue of concern when conducting its operations.

V. Conclusion

The United States government has displayed two contradictory viewpoints on the value of a citizen's personal privacy. Absurdly, both of these attitudes have been used to justify government secrecy. On the one hand, privacy is being used increasingly as the justification for withholding government-held documents under FOIA Exemptions 6 and 7(C), thus preventing public knowledge of the governmental operations discussed in those documents. Conversely, privacy concerns are powerless in reducing the secrecy of the surveillance state. Hence, a government that praises privacy as a reason for withholding documents ignores that same value when collecting personal data on citizens.

There are two possible solutions for this conundrum. Given the surveillance state's disdain for privacy, the judiciary could place less credence in agency denials of FOIA requests in which personal privacy has been cited, thus enabling more disclosure of documents that can inform the public on how the government does business. Or, the judiciary could recall the government's concern for personal privacy in FOIA denials as a reason to reject the security establishment's reasoning for extending its electronic surveillance operations. Either of those options would make a certain logical sense, but perhaps this is a facetious dichotomy, as any sort of dispute over

---

[197] *See* Ohm, *supra* note 11, at 1354.

the government's invasion of privacy could be considered on a case-by-case basis. It is important to note that privacy and security are not a zero-sum game, as it is possible to have both.[198] Or as this article suggests, it may be possible to have both full disclosure of government-held documents and relief from invasive surveillance.

The American government, however, has invoked the spurious "privacy or security" dichotomy in two contradictory ways. First, privacy values prevent public understanding of government-held documents; second, citizens' understanding of their loss of privacy is prevented by the need for security. Either way, the public knows less about governmental operations, and this violates the pro-transparency philosophy of FOIA, which Congress justified in 1966 by citing the need for a broad philosophy of open government and the democratic ideal of an informed citizenry. As noted by the House of Representatives, access to government-held documents is essential because the "intelligence of the electorate varies as the quantity and quality of its information varies."[199] The Senate also observed that "it is only when one further considers the hundreds of departments, branches, and agencies which are not directly responsible to the people, that one begins to understand the great importance of having an information policy of full disclosure."[200]

In the words of Paul Ohm, "If we woke up tomorrow in a world without privacy, we might also find ourselves in a world without constitutional protection from new, invasive police powers. This bleak scenario is not science fiction, for tomorrow we will likely wake up in that world."[201] While Ohm opined that privacy is collapsing under the sheer invasiveness of the surveillance state, the present article also argues that privacy is in danger of disappearing as a virtue because American citizens have been prevented from learning about how it is being infringed. The American government abuses the spirit of privacy in two different ways to justify two ostensible abuses of power–

---

[198] *See* SOLOVE, *supra* note 134, at 33-37.
[199] *See* H.R. REP. NO. 89-1497, at 12 (1966).
[200] *See* S. REP. NO. 89-813, at 38 (1965).
[201] *See* Ohm, *supra* note 11, at 1310.

maintaining secrecy through the nondisclosure of documents and expanding the questionable surveillance powers of the national security and law enforcement establishments. This contradictory pattern violates both the pro-disclosure spirit of FOIA and the spirit of agency discretion toward personal information that fueled the Privacy Act.[202]

While privacy has become *exceptional* when the American government seeks to keep agency documents secret, privacy has been treated as *unexceptional* by the surveillance state. This is an awkward, contradictory, and two-faced stance on an important social value. More specifically, governmental transparency is defeated by privacy concerns in FOIA jurisprudence, while privacy concerns are defeated by the non-transparency of the surveillance state. Both of these serve as forms of nondisclosure; the former is literal and the latter is *de facto*. Agencies that withhold requested documents, and other agencies that conduct invasive electronic surveillance, have escaped full accountability by misusing the spirit of privacy in disingenuous fashions. The government cannot have it both ways—if it claims to care about personal privacy some of the time, it should do so all the time.

---

[202] *See Overview of the Privacy Act of 1974*, *supra* note 71.