Suffolk Journal of Trial and Appellate Advocacy

Volume 26 | Issue 2 Article 9

1-1-2021

Constitutional Law—Narrowly Reading Law Enforcement Activity Exception to Privacy Act in Favor of Privacy Rights—Garris v. FBI, 937 F.3d 1284 (9th Cir. 2019)

Megan Ryan
Suffolk University Law School

CONSTITUTIONAL LAW—NARROWLY READING LAW ENFORCEMENT ACTIVITY EXCEPTION TO PRIVACY ACT IN FAVOR OF PRIVACY RIGHTS—*GARRIS V. FBI*, 937 F.3D 1284 (9TH CIR. 2019)

One of the core civil rights granted by the Constitution is the First Amendment's protection of free speech and expression.[1] To further safeguard First Amendment rights and protect citizens' right to privacy, Congress passed the Privacy Act in 1974, which states in part: "[e]ach agency that maintains a system of records shall . . . maintain no record describing how any individual exercises rights guaranteed by the First Amendment . . . unless pertinent to and within the scope of an authorized law enforcement activity."[2] In *Garris v. FBI*,[3] the Ninth Circuit considered whether a government agency can maintain such a record, if its creation is permissible under the Privacy Act's law enforcement activity exception.[4] The court held that "unless a record is pertinent to an ongoing authorized law enforcement activity, an agency may not maintain [this type of record]" under the law enforcement activity exception of the Privacy Act.[5]

---

[1] *See* U.S. CONST. amend. I (stating "Congress shall make no law . . . abridging the freedom of speech . . . ."); *see also* Nicholas G. Karambelas, *Where the First Amendment Comes From*, 50 MD. B.J. 4, 10-13 (2017) (describing First Amendment and reasoning behind freedom of expression).

[2] *See* 5 U.S.C. § 552a(e)(7) (restricting record maintenance regarding citizens' exercise of their First Amendment rights); *see also* S. REP. NO. 93-1183, at 6916 (1974) (explaining purpose of Privacy Act as "promot[ing] governmental respect for the privacy of citizens by requiring all departments and agencies . . . to observe certain constitutional rules in the computerization, collection, management, use, and disclosure of personal information about individuals.")

[3] 937 F.3d 1284 (9th Cir. 2019).

[4] *See id.* at 1288 (introducing issue of first impression in Ninth Circuit).

[5] *See id.* at 1300 (holding continued maintenance of records must be relevant to ongoing law enforcement activity). The Ninth Circuit stated:

> [W]e hold that to maintain a record, the government must demonstrate that the maintenance of the record is pertinent to a specific authorized law enforcement activity. We want to be exceedingly clear. We are *not* holding that whenever an agency closes an investigation, the agency must expunge the file because the law enforcement activity for which the record was created (or received) has ended. What we are holding is that, if the investigation is closed (or even if it is not), and if the government cannot articulate a sufficient law enforcement activity to which the *maintenance* of the record is pertinent, the maintenance of the record violates the Privacy Act. The reason for maintenance, so long as it is valid and not pretextual, need not be the same reason the record was created.
>
> *Id.*

Eric Anthony Garris is the founder, managing editor, and webmaster of Antiwar.com, a news platform serving as an alternative outlet to mainstream media.[6] In 2011, Garris learned of a memo, created in 2004 ("2004 Memo") by the Federal Bureau of Investigation's ("FBI") Newark, New Jersey office, which detailed an investigation into Antiwar.com.[7] The FBI created the 2004 Memo after the agency discovered a twenty-two-page Excel spreadsheet from October 2001, which had been posted on Antiwar.com and appeared to be a potential FBI watchlist.[8] Although FBI analysts recommended in the 2004 Memo that the FBI's San Francisco Field Office further monitor Antiwar.com and open a preliminary investigation to determine if the website was a threat to national security, the San Francisco Field Office declined this recommendation and ultimately determined that Antiwar.com was not a threat.[9] The 2004 Memo included Anti-

---

[6] *See id.* at 1288 (describing Garris's role at Antiwar.com and purpose of website as "'an anti-interventionalist, pro-peace,' non-profit news website"). Antiwar.com's mission is "to publish news, information and analysis on the issues of war and peace, diplomacy, foreign policy, and national security" and the website "self-describes as advocating for 'non-interventionism.'" *Id.* Antiwar.com's "about us" page further describes its mission:

> This site is devoted to the cause of non-interventionism and is read by libertarians, pacifists, leftists, "greens," and independents alike, as well as many on the Right who agree with our opposition to imperialism. . . . Our politics are libertarian: our opposition to war is rooted in Randolph Bourne's concept that "War is the health of the State." With every war, America has made a "great leap" into statism, and as Bourne emphasized, "it is during war that one best understands the nature of that institution [the State]." At its core, that nature includes an ever increasing threat to individual liberty and the centralization of political power.

About Us, MISSION, ANTIWAR.COM, https://www.antiwar.com/who.php (last visited Dec. 1, 2020); *see also* Lyndsey Wajert, *RFCP Analysis: Court Orders FBI to Expunge Website Records Under Privacy Act*, REPORTERS COMM. FOR FREEDOM OF THE PRESS (Jan. 16, 2020), https://www.rcfp.org/fbi-antiwar-privacy-act/ (reporting on *Garris* decision); Antiwar Staff, *Justin Raimondo, RIP (1951-2019)*, ANTIWAR.COM (June 27, 2019), https://original.antiwar.com/antiwar_staff/2019/06/27/justin-raimondo-rip-1951-2019/ (paying tribute to Justin Raimondo—prominent libertarian who co-founded Antiwar.com). Justin Raimondo was the former editorial director of Antiwar.com and a party to the suit against the FBI; sadly, he passed away in 2019. *See* Antiwar Staff, *supra* note 6.

[7] *See Garris*, 937 F.3d at 1289 (noting Garris learned about memo in August 2011 from partially redacted version online).

[8] *See id.* at 1288-89 (describing discovery of possible FBI watch list on Antiwar.com). In March 2004, the FBI warned all field offices that a post-9/11 suspect list called "Project Lookout" had been posted on the internet with identifying information of people of interest. *Id.* at 1288. An FBI agent then discovered the Excel spreadsheet on Antiwar.com, which contained names and identifying information. *Id.* After further investigation, a second twenty-two-page spreadsheet was discovered on Antiwar.com dated May 2002 and was marked "FBI SUSPECT LIST." *Id.*

[9] *See id.* at 1289 (noting recommendation to San Francisco Field Office and declination to investigate further). The FBI's San Francisco Field Office noted that the information on Antiwar.com was public information and that Garris was exercising his right to free speech. *Id.*

war.com's mission and information on Garris—specifically, his political views and his "articles, opinions, statements, or speeches[.]"[10]

In May 2013, Garris's request that the FBI expunge all records that detailed his First Amendment activities was denied; he subsequently filed a complaint and alleged that the creation and maintenance of the 2004 Memo violated the law enforcement activity exception of the Privacy Act.[11] Additionally, Garris sought disclosure of the FBI's documents about him under the Freedom of Information Act.[12] The United States District Court for the Northern District of California granted summary judgment to the FBI for Garris's Privacy Act claim; however, because of Garris's continued Freedom of Information Act claims, he later learned of the Halliburton Memo ("Halliburton Memo").[13] The Halliburton Memo, created in 2006 by the FBI's Oklahoma City Field Office, contained information about an annual Halliburton shareholders' meeting that Antiwar.com had previously posted information about.[14] Garris consequently moved for reconsideration of his Privacy Act claims, given the new information cited in the Halliburton Memo; however, the district court denied his motion for reconsideration and granted summary judgment for the FBI.[15] Garris appealed his Privacy Act claims, and the Ninth Circuit held that a record must be pertinent to be maintained as an ongoing law enforcement activity.[16] Accordingly, the Ninth Circuit concluded that the 2004 Memo must be expunged, but ruled that the Halliburton Memo was pertinent to an ongoing law enforcement activity and therefore could be maintained.[17]

In 1974, Congress enacted the Privacy Act, with the primary goal to protect privacy rights in response to both computer technology advancements and concerns of governmental abuse in the "computerization, collection, management, use, and disclosure of personal information about

---

[10] *See id.* (detailing information included in 2004 Memo). The 2004 Memo had the subject "threat assessment . . . Eric Anthony Garris [and] www.antiwar.com" and discussed both the watch lists and Antiwar.com's mission. *Id.* Some of the information included in the 2004 Memo was the result of law enforcement database searches, such as Lexis Nexis, for Garris and Antiwar.com. *Id.*

[11] *See id.* at 1290 (outlining procedural background of case).

[12] *See Garris*, 937 F.3d at 1290 (listing legal claims Garris brought against FBI).

[13] *See id.* at 1290-91 (indicating how Garris learned of Halliburton Memo from documents disclosed by FBI).

[14] *See id.* at 1289-90 (detailing Halliburton Memo's contents and relation to Antiwar.com). The Halliburton Memo described the Halliburton company, its contracts and affiliations, and information about the shareholder's meeting. *Id.* at 1289.

[15] *See id.* at 1291 (explaining procedural history of Garris's district court claims).

[16] *See id.* at 1288 (stating Ninth Circuit's holding regarding law enforcement activity exception to Privacy Act).

[17] *See Garris*, 937 F.3d at 1291 (describing procedural history and Ninth Circuit's holding).

individuals."[18] The Privacy Act sets out to accomplish this goal in several major ways; first, the Act requires agencies to give detailed information about their personal data banks, information systems, and computer resources.[19] Second, agencies must abide by standards formed to: protect individuals' privacy and due process rights; uphold the handling and processing of information in data banks; and preserve information security and information systems.[20] Third, to truthfully restrain agencies' handling of

[18] *See* S. REP. NO. 93-1183, at 6916 (1974) (summarizing Privacy Act's purpose). The Privacy Act aims to increase accountability of government agencies by ensuring that they abide by principles of fairness and privacy, and only use Americans' personal information in accordance with the legitimate needs of the government. *Id.* at 6916-17; *see also* Eric C. Surette, Annotation, *Prohibition of Federal Agency's Keeping of Records on Methods of Individual Exercise of First Amendment Rights, Under Privacy Act of 1974 (5 U.S.C.A. § 552a(e)(7))*, 20 A.L.R. FED. 2d 437, §2 (2007) (discussing primary purpose of Privacy Act as providing individuals more control over information about themselves); Miriam Schneider, Note, *Military Spying in the United States: When It Is Not Your Neighbor Knocking At Your Door, Where Do You Turn?*, 7 CARDOZO J. CONFLICT RESOL. 199, 217 (2005) (listing factors leading to Privacy Act, notably development of technology and computers); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 40 (2003) ("A stated objective of the Privacy Act was to restrict the government's use of technology to invade privacy interests . . . ."); Steven W. Becker, Comment, *Maintaining Secret Government Dossiers on the First Amendment Activities of American Citizens: The Law Enforcement Activity Exception to the Privacy Act*, 50 DEPAUL L. REV. 675, 678-83 (2000) [hereinafter Becker, *Dossiers*] (highlighting several factors contributing to passage of Privacy Act). When introducing the bill, Senator Samuel J. Ervin, Jr. noted that, "Congress must act before sophisticated new systems of information gathering and retention are developed . . . [because] once they go into operation, it is too late to correct our mistakes or supply our oversight." *See* Becker, *Dossiers*, *supra* note 18, at 679. Governmental abuses driving the concern for protecting personal data and information arose from allegations of improper handling of information in the Watergate investigations, the FBI's surveillance of political and religious groups under its COINTELPRO operation, the DOJ's warrantless wiretapping of citizens, investigations in the McCarthy era after the Cold War, the IRS's improper monitoring of tax records for political purposes, and the Army's surveillance of civilians. Becker, *Dossiers*, *supra* note 18, at 680-83. *See generally Surveillance Under the USA/PATRIOT Act*, ACLU, https://www.aclu.org/other/surveillance-under-usapatriot-act (last visited Dec. 1, 2020) [hereinafter PATRIOT Act, ACLU] (providing information on PATRIOT Act and government surveillance of American citizens). The PATRIOT Act was passed in response to the September 11, 2001 attacks, and was described by the ACLU as "an overnight revision of the nation's surveillance laws that vastly expanded the government's authority to spy on its own citizens." *See* PATRIOT Act, ACLU, *supra* note 18. According to the ACLU, the PATRIOT Act appears consistent with the government abuses that triggered the 1974 Privacy Act, as it provided "unchecked government power to rifle through individuals' financial records, medical histories, Internet usage, bookstore purchases, library usage, travel patterns, or any other activity that leaves a record." *See* PATRIOT Act, ACLU, *supra* note 18.

[19] *See* S. REP. NO. 93-1183, at 6917-19 (1974) (outlining ways Privacy Act meets its purposes). The Act created a new Privacy Commission, which maintains and publishes information for the public and carries out duties aimed at protecting privacy and individual rights. *Id.* Agencies that do not disclose the requisite information are penalized. *Id.*

[20] *See id.* at 6917-18 (explaining standards and outlining requirements for agencies to abide by). The information-gathering standards include: requiring the personal information that agencies collect and maintain be "relevant and necessary[;]" obliging this personal information be collected directly from the source when possible, in order to prevent inaccuracies; informing whether

personal data, the Act provides for a citizen's right "to be told upon request whether or not there is a government record on him or her, to have access to it, and to challenge it with a hearing upon request."[21] Lastly, Congress required the Privacy Protection Commission, established under the Privacy Act, to complete a study of the major information systems of governmental agencies and recommend changes to protect individuals' privacy.[22] While the Privacy Act aims to protect the privacy of individuals if a record is "pertinent to and within the scope of an authorized law enforcement activity," the protections preventing agencies from maintaining records "describing how any individual exercises rights guaranteed by the First Amendment" are inapplicable.[23]

While the Privacy Act clearly states an exception to maintaining records related to First Amendment activities, the appellate courts have varied in their interpretation of the law enforcement activity exception.[24] In

"disclosure is mandatory or voluntary[;]" and mandating a "strict reviewing process" before establishing any program for information on how people exercise First Amendment rights. *Id.* at 6917. Agencies must ensure, among other things, that: (1) the information they have is "accurate, complete, timely and relevant[;]" (2) they "refrain from disclosing [information] unless necessary for employee duties" or proper consent or laws allow; (3) they keep proper records of people and organizations with access to different systems and files; (4) rules of conduct are established regarding the legal and ethical obligations surrounding the computerization and handling of personal data; (5) they do "not sell or rent" information; and (6) proper safeguards are in place ensuring the security and confidentiality of data and systems. *Id.* at 6917-18.

[21] *See id.* at 6918 (explaining methods for administrative and judicial oversight and civil remedies for violations). Congress established the Privacy Protection Commission, an independent agency, to: investigate and report violations of the Privacy Act; assist agencies implementing the Privacy Act; and alert the President and Congress to proposed programs and data banks with the potential to violate the Privacy Act. *Id.* at 6918.

[22] *See id.* at 6918 (1974) (detailing Privacy Protection Commission's mandate to recommend changes to protect individuals' privacy).

[23] *See* 5 U.S.C. § 552(e)(7) (explaining law enforcement activity exception to Privacy Act); *see also* S. REP. NO. 93-1183, at 6938 (demonstrating how law enforcement typically creates files while investigating or anticipating criminal activity).

> [I]nformation generally maintained by law enforcement agencies are intelligence, or investigative files. These files contain highly sensitive and usually confidential information collected by law enforcement officers in anticipation of criminal activity, such as by organized crime figures, or in the course of investigating criminal activity which has already occurred. It was the Committee's judgment, shared by most criminal justice privacy experts and reflected in the pending criminal justice privacy legislation, that all of the provisions of title II of S. 3418 could not be applied to such sensitive information.

S. REP. NO. 93-1183, at 6938; Jill I. Goldenziel et al., *The New Fighting Words?: How U.S. Law Hampers the Fight Against Information Warfare*, 22 U. OF PA. J. CONST. L. 81, 118 (2019) ("Requiring a blanket prohibition on surveillance and recording until 'the agency was investigating a specific offense or a specific person' would severely undermine agency activities.")

[24] *See* Becker, *Dossiers*, *supra* note 18, at 699 ("Various appellate courts have adopted different standards in construing subsection (e)(7)'s law enforcement activity exception.")

Clarkson v. IRS, the Eleventh Circuit held that the IRS violated the Privacy Act "to the extent that the IRS has engaged in the practice of collecting protected information, unconnected to any investigation of past, present or anticipated violations of the statutes which it is authorized to enforce."[25] Conversely, the Sixth Circuit in *Jabara v. Webster* allowed the FBI's maintenance of records on Jabara—despite finding that the records were not related to any specific criminal act—and held that the law enforcement activity exception will be too narrowly interpreted if it only requires records to relate to an investigation of criminal activity.[26] Similar to the Sixth Circuit, the Third Circuit, in *Patterson v. FBI*, also interpreted the law enforcement activity exception as "requir[ing] agencies 'to demonstrate that any and all records maintained on an individual's exercise of First Amendment rights are *relevant* to an authorized law enforcement activity of the agency, and that there exists a sufficient basis for the maintenance of such records.'"[27] The D.C. Circuit held in *J. Roderick MacArthur Foundation v. FBI* that "if the information was pertinent to an authorized law enforcement activity when the agency collected the information," the agency was not prohibited from maintaining records about an individual's First Amendment activities, and did not need to expunge the records when they were no longer pertinent to law enforcement activity.[28] While both the

---

[25] *See* Clarkson v. IRS, 678 F.2d 1368, 1375 (11th Cir. 1982) (remanding issue under (e)(7) of Privacy Act to determine purpose of surveillance activities). Clarkson was involved in many organizations to protest the federal tax system; in 1979, he was the keynote speaker at a meeting in Georgia to plan the 1979 Tax Protest Day demonstration. *Id.* at 1369-70. Undercover IRS agents attended the meeting, and upon learning of their attendance, Clarkson initiated a series of complaints against the IRS, including a complaint that the IRS violated his rights under the Privacy Act. *Id.* at 1370.

[26] *See* Jabara v. Webster, 691 F.2d 272, 280 (6th Cir. 1982) (finding district court too narrowly construed law enforcement activity exemption). The FBI was investigating Jabara for his involvement in Arab causes. *Id.* at 273. The FBI maintained and disseminated information obtained from physical surveillance by agents and informants, inspection of his bank records, warrantless electronic surveillance, and interviews of others with knowledge about Jabara. *Id.*

[27] *See* Patterson v. FBI, 893 F.2d 595, 602-03 (3d. Cir. 1990) (quoting Patterson v. FBI, 705 F. Supp. 1033, 1043 (D.N.J. 1989)) (agreeing with district court's interpretation of law enforcement activity exception). As part of a sixth-grade school project to write a world encyclopedia, Patterson wrote to 169 countries requesting information. *Id.* at 597. The FBI opened a file on Patterson due to the volume of international mail he received. *Id.* The FBI monitored Patterson's activities from 1983 until 1985, and his family reported receiving mail in damaged condition and hearing strange background noises on their telephone. *Id.* at 598. In response to Patterson's (e)(7) claim under the Privacy Act, the Third Circuit found that the FBI's records were relevant as an authorized law enforcement activity. *Id.* at 603.

[28] *See* J. Roderick MacArthur Foundation v. FBI, 102 F.3d 600, 605 (D.C. Cir. 1996) (holding law enforcement may maintain records if pertinent to law enforcement activity when collected). Lindblom, in his capacity as president of the J. Roderick MacArthur Foundation, would meet with foreign leaders and political figures because the Foundation worked with organizations on political, social, and economic issues. *Id.* at 601. When Lindblom discovered the FBI had a

Seventh and Eighth Circuits have had this issue before them, neither have adopted a specific standard for interpreting the law enforcement activity exception.[29]

In 1986, the Ninth Circuit interpreted the law enforcement activity exception of the Privacy Act in *MacPherson v. IRS*—the only decision in the Ninth Circuit prior to *Garris*.[30] As part of its surveillance of the tax protester movement, the IRS attended several events at which MacPherson spoke.[31] In an effort to identify leaders of the tax protest movement and determine protester strategies, the IRS maintained notes and recordings of MacPherson's speeches in a file titled "Tax Protest Project File" in two IRS offices, and later distributed the files to three more IRS offices, the Department of Justice, and additional third parties.[32] Notably, IRS surveillance of MacPherson did not uncover any illegal activity on his part, nor was he suspected or accused of any past, present, or anticipated illegal conduct.[33] Despite this, the Ninth Circuit affirmed the district court's finding in favor of the IRS, and noted that there was no indication that the IRS planned to use the records for any purpose other than to give a complete picture of the conference where MacPherson spoke.[34] Distinct from the circuits that have adopted a rule interpreting the law enforcement activity exception, the Ninth Circuit "decline[d] to fashion a hard and fast standard[,]" and instead "elect[ed] to consider the factors for and against the maintenance of such records of First Amendment activities on an individual, case-by-case basis."[35]

---

file on him because of his involvement with the Foundation, he filed a complaint under the Privacy Act—but the district court decided in the FBI's favor. *Id.* at 601-02.

[29] *See* Bassiouni v. FBI, 436 F.3d 712, 724 (7th Cir. 2006) ("Like our sister circuits, we do not believe that the circumstances presented to us here required us to determine the precise limits of the term 'law enforcement activity.'"); Becker, *Dossiers*, *supra* note 18, at 705-06 (noting decision in *Wabun-Inini v. Sessions*, 900 F.2d 1234, 1245-46 (8th Cir. 1990), "[t]he court did not adopt a specific standard of interpretation and stated that it preferred 'to delay a closer scrutiny of the law enforcement exemption until the issue is more carefully framed and necessary to the decision.'")

[30] *See* MacPherson v. IRS, 803 F.2d 479, 480-85 (9th Cir. 1986) (analyzing section (e)(7) of Privacy Act in relation to MacPherson's claims); Garris v. FBI, 937 F.3d 1284, 1296 (9th Cir. 2019) (stating *MacPherson* is only opinion interpreting section (e)(7) of Privacy Act).

[31] *See MacPherson*, 803 F.2d at 480 (outlining undisputed facts relevant to issue on appeal).

[32] *See id.* (describing IRS tracking of MacPherson's First Amendment activity).

[33] *See id.* (noting illegal activity was not relevant to MacPherson's surveillance).

[34] *See MacPherson*, 803 F.2d at 484-85 (affirming district court's finding in favor of IRS). The Ninth Circuit noted that MacPherson gave his speeches in public, and anyone willing to pay for the price of the tape could access them. *Id.* at 484. Additionally, MacPherson even acknowledged in a speech that there may be IRS agents in the audience. *Id.*

[35] *See id.* at 484 (electing to adopt case-by-case standard due to strong policy arguments on both sides). The court discussed the policy considerations, noting that on one hand "even 'incidental' surveillance and recording of innocent people . . . may have the 'chilling effect' on those

In 2019, the Ninth Circuit in *Garris v. FBI* considered whether the Privacy Act required the FBI's 2004 Memo and Halliburton Memo to be "pertinent to an ongoing law enforcement activity to be maintained."[36] The court looked to the text of the Privacy Act, and the definitions of its specific words used, and determined that because the statute defined "maintain" as "maintain, collect, use, or disseminate," the word "maintain" in the Privacy Act can be read "as it is, or replaced with 'collect' (or 'use,' or 'disseminate')."[37] This analysis of statute's language led to the court's conclusion that "the most reasonable reading of the statute as a whole is that the record must be pertinent to an authorized law enforcement activity both 'at the time of gathering, i.e., collecting, [and] at the time of keeping, i.e., maintaining.'"[38] To support its conclusion, the court referred to the purpose of the Privacy Act, noting that Congress was particularly concerned with preventing "both collection *and* retention of records."[39] Furthermore, the court compared its conclusion to *MacPherson*—its only other opinion discussing the law enforcement exception—and found it consistent with the *MacPherson* court's narrow reading of the law enforcement activity exception because it "better serves the goal of privacy."[40]

The court disagreed with the FBI's stance that records only need to be pertinent to an authorized law enforcement activity at the time of collection; rather, the court noted that (1) accepting this position would "read the word 'maintain' out of the statute," (2) a reading of the statute "that divorces the authorized law enforcement activity clause from the verb" does not work when reading the statute with the verbs "disseminate" or "use" instead of "maintain," and (3) "use" being included in the statute's definition of "maintain" indicates the regulation of records that have already been

---

rights," and on the other hand, legitimate investigation and surveillance can be necessary in order to be "certain that political and religious activities are not used as a cover for subversive activities." *Id.* at 484.

[36] *See* Garris v. FBI, 937 F.3d 1284, 1294 (9th Cir. 2019) (identifying issue of first impression). In addressing this issue of whether under the Privacy Act a record needs to be pertinent to an ongoing law enforcement activity to be maintained, the Ninth Circuit assumed that the record's creation did not violate the Privacy Act. *Id.*

[37] *See* 5 U.S.C. § 552(e)(7) (stating law enforcement activity exception to Privacy Act); *Garris*, 937 F.3d at 1294-95 (examining definitions of "maintain" and "collect" and their reading in statute). The court also looked to the Oxford English Dictionary's definition of "maintain" and "collect" to ascertain the plain meaning of the words. *Garris*, 937 F.3d at 1294.

[38] *See Garris*, 937 F.3d at 1295 (stating requirement of current "law enforcement activity" for record to be pertinent).

[39] *See id.* at 1295-96 (noting purpose of Privacy Act and congressional intent).

[40] *See id.* at 1296 (quoting MacPherson v. IRS, 803 F.2d 479, 482 (9th Cir. 1986)) (comparing holding to *MacPherson*). The Ninth Circuit also noted its conclusion aligned with two Seventh Circuit decisions, *Becker v. IRS*, 34 F.3d 398 (7th Cir. 1994) and *Bassiouni v. FBI*, 436 F.3d 712 (7th Cir. 2006). *Id.*

created.[41] The court recognized that, while the FBI's same argument was ultimately upheld in the D.C. Circuit's decision in *J. Roderick MacArthur Foundation*, the court ultimately disagreed with the D.C. Circuit's reasoning and interpretation of the statute's language; the court further remarked that, when Congress means "*collection*[,]" and not "maintenance" or "retention," it knows how to explicitly state so.[42] Relying on its conclusion that the law enforcement activity exception to the Privacy Act applies to both collection and maintenance of records, the court found that the 2004 Memo was not pertinent to an authorized law enforcement activity because the FBI's threat assessment "turned up nothing more than protected First Amendment activity[,]" and had "at best only speculative relevance to an unstated law enforcement purpose."[43] Conversely, the court found that the Halliburton Memo was pertinent to an authorized law enforcement activity because the memo: was not under Garris's or Antiwar.com's name; was created to provide information on the annual shareholders meeting that local law enforcement was required to prepare for; and "only incidentally include[d] protected First Amendment activity."[44]

The Ninth Circuit's decision in *Garris v. FBI* was a step forward towards safeguarding citizens' privacy and protecting ed First Amendment activity—an issue that has grown more pressing with recent technological advances.[45] The requirement, affirmed in this decision, of an authorized law enforcement activity in order to both collect and maintain records aligns with the purpose of the Privacy Act, which is to "promote governmental respect for the privacy of citizens."[46] Without this check that agen-

---

[41] *See id.* at 1295-97 (delineating flaws in FBI's argument).

[42] *See id.* at 1297 (emphasis added) (explaining reasons for disagreement with D.C. Circuit's decision that "the record itself, must be pertinent to an authorized law enforcement activity" (quoting J. Roderick MacArthur Found. v. FBI, 102 F.3d 600, 603 (D.C. Cir. (1996)))).

[43] *See Garris*, 937 F.3d at 1298-99 (applying conclusion on law enforcement activity exception to 2004 Memo). The court compared the contents of the 2004 Memo to the records in *MacPherson*, and noted that the record in *MacPherson* was related to a larger ongoing undertaking and was in a "general tax protestor file, *not* under MacPherson's name[;]" whereas, the 2004 Memo was specifically filed under Garris' name and not part of a "larger, valid investigation." *Id.* at 1298-99.

[44] *See id.* at 1300 (concluding Halliburton Memo was within law enforcement activity exception).

[45] *See* Nehf, *supra* note 18, at 10 ("[L]ack of control over information has long been a concern of privacy advocates.") "[M]ost recognize and appreciate the many benefits of data storage and information technologies . . . but [] are concerned about how personal information might be used." *Id.* at 9; *see also* Schneider, *supra* note 18, at 217 (explaining computers' "unforeseen potential to collect, and . . . an almost unlimited capacity to retain information"); Becker, *Dossiers*, *supra* note 18, at 741 (emphasizing potential consequences of failing to protect First Amendment freedoms).

[46] *See* S. REP. NO. 93-1193, *supra* note 18, at 6916 (noting purpose of Privacy Act); *see also* sources cited *supra* note 18 (discussing intent of Privacy Act).

cies require records to be pertinent to law enforcement activity, both at collection and while retained, fundamental rights granted by the Constitution could be threatened, resulting in a society not unlike a police state—a concept "truly frightening to a society nurtured on freedom."[47] A potential threat to free speech and privacy rights occurred with the enactment of the PATRIOT Act in 2001, which increased the government's surveillance powers in record searches, secret searches, intelligence searches, and "trap and trace" searches.[48] With the existence of legislation like the PATRIOT Act, the decision in *Garris* is all the more substantial as it upholds citizens' rights as well as maintains checks and balances on the government.[49]

A common concern regarding the Ninth Circuit's conclusion is that requiring all records to be related to a pertinent law enforcement activity could hinder the work of the U.S. government in its national security efforts.[50] The law enforcement activity exception, however, does not necessarily forbid incidental surveillance of innocent people because it "would be administratively cumbersome and damaging to the completeness and accuracy of the agency records[;]" consequently, it seems with a legitimate national security threat, the government has more flexibility with national security efforts.[51] Furthermore, if the U.S. government was concerned with managing national security threats without infringing upon citizens' rights,

---

[47] *See* Becker, *Dossiers*, *supra* note 18, at 738-41 (describing impact if citizens do not have the freedom to meaningfully scrutinize retained, governmental records); *see also* Nehf, *supra* note 18, at 23-29 (explaining potential harm to individuals resulting from data collection and sharing).

[48] *See* PATRIOT Act, ACLU, *supra* note 18 (detailing government's increased surveillance powers). Under the PATRIOT Act, the government can look at records held by a third party on an individual's activity and can search private property without notice to the owner. *Id.* The PATRIOT Act expanded "a narrow exception to the Fourth Amendment that had been created for the collection of foreign intelligence information" and "another Fourth Amendment exception for spying that collects 'addressing' information about the origin and destination of communications, as opposed to the content." *Id.*

[49] *See id.* ("PATRIOT Act vastly expanded the government's authority to spy on its own citizens, while simultaneously reducing checks and balances on those powers like judicial oversight, public accountability, and the ability to challenge government searches in court."); Garris v. FBI, 937 F.3d 1284, 1296 (9th Cir. 2019) ("In fact, the Act was 'designed to set in motion a long-overdue evaluation of the needs of the Federal government to acquire *and retain* personal information on Americans, by requiring stricter review within agencies of criteria for *collection and retention*' of such information.")

[50] *See* Goldenziel & Cheema, *supra* note 23, at 85-86, 118-20 (arguing U.S. laws must reform to protect national security).

[51] *See* MacPherson v. IRS, 803 F.2d 479, 484 (9th Cir. 1986) (explaining incidental surveillance cannot be forbidden); Goldenziel & Cheema, *supra* note 23, at 118 (noting "[c]ourts in Privacy Act cases have found that national security concerns generally prevail over concerns about the potential of the government's action to chill speech[.]"). Therefore, it seems the government's hands would not necessarily be tied with a legitimate national security threat. *See* Goldenziel & Cheema, *supra* note 23, at 118; Nehf, *supra* note 18, at 4 n.12 (noting recent trend favoring strength of law enforcement at expense of individual privacy).

lawmakers could carefully improve existing legislation to achieve such a goal.[52] Some scholars suggest broadening the scope of the Privacy Act's law enforcement activity exception to prevent agencies from maintaining records, which describe how individuals exercise First Amendment rights unless pertinent to and within the scope of a specific national security purpose or an authorized law enforcement activity.[53] Changes to the exception in favor of national security should, however, go through extensive legislative review, be worded carefully and specifically to prevent broad interpretation of key terms, and require stringent judicial review whenever government agencies access information about citizens' First Amendment speech.[54]

---

[52] *See* Goldenziel & Cheema, *supra* note 23, at 135-38 (detailing how surveillance laws could be improved while still considering citizens' rights). In contrast to the PATRIOT Act—which allowed for unrelated provisions to be included—improvements to the Privacy Act and other surveillance laws should be tailored to specific national security concerns. *Id.* at 135.

[53] *See id.* at 136 (recommending legislators grant agencies power to access information necessary to secure national security).

[54] *See* PATRIOT Act, ACLU, *supra* note 18 (criticizing PATRIOT Act). Any changes in favor of national security to the Privacy Act law enforcement activity exception should learn from the mistakes of the PATRIOT Act. *See id.* The PATRIOT Act drew much criticism due to its hasty enactment and "[m]any Senators complained that they had little chance to read it, much less analyze it, before having to vote." *Id.* Furthermore, any potential changes to the Privacy Act to increase national security should be as transparent as possible with the rest of the government and the public, as opposed to the PATRIOT Act, which did not have much accountability per the ACLU:

> Attempts to find out how the new surveillance powers created by the Patriot Act were implemented during their first year were in vain. In June 2002 the House Judiciary Committee demanded that the Department of Justice answer questions about how it was using its new authority. The Bush/Ashcroft Justice Department essentially refused to describe how it was implementing the law; it left numerous substantial questions unanswered and classified others without justification. In short, not only has the Bush Administration undermined judicial oversight of government spying on citizens by pushing the Patriot Act into law, but it is also undermining another crucial check and balance on surveillance powers: accountability to Congress and the public.

Id.; Goldenziel & Cheema, *supra* note 23, at 135-37 (explaining mistakes of PATRIOT Act and suggesting model used by Foreign Intelligence Surveillance Act (FISA)). The PATRIOT Act has been observed as being "like a Christmas tree, where provisions with other purposes are attached without much connection, for other powers that law enforcement agencies and national security agencies would like to wield," so any changes to the Privacy Act should aim to not make the same mistakes by articulating "a specific national security purpose that any related surveillance would support." Goldenziel & Cheema, *supra* note 23, at 135. The FISA allows for the "surveillance of foreign agents without unduly infringing on the civil liberties of U.S. persons." Goldenziel & Cheema, *supra* note 23, at 136. The FISA model permits government surveillance if a judge finds probable cause that the target is a foreign power, and the facility is used by the target. Goldenziel & Cheema, *supra* note 23, at 136. The judge can consider the target's activities and related facts and circumstances, but "cannot accept the government's assertion that someone is an agent of a foreign power solely based on activities protected by the First Amendment." Goldenziel & Cheema, *supra* note 23, at 136.

Overall, the Ninth Circuit's decision is promising for all citizens who value First Amendment freedoms, particularly those who are vocal about frequently censored issues.[55] Journalists, for example, have often been monitored or surveilled after reporting on information that is classified or leaked, or expressing an opinion unfavorable to the government; therefore, the Ninth Circuit's decision in *Garris v. FBI* provides some comfort as the law enforcement activity exception to the Privacy Act also protects the freedom of the press.[56] While the Ninth Circuit's holding in *Garris* leans more conservatively in favor of protecting privacy rights, the Ninth Circuit's ultimate ruling created to review the factors on a case-by-case basis, leaves room for potential future unfavorable outcomes for citizens.[57] As this decision only affects the Ninth Circuit, perhaps the Supreme Court will address this "important but rarely considered provision of the Privacy Act," consider differing interpretations among the circuits, and the impact on citizens' highly valued First Amendment rights.[58]

Garris v. FBI considered whether the law enforcement activity exception to the Privacy Act allowed for records that were permissibly created to continue to be maintained by a government agency. In alignment

---

[55] *See* Wajert, *supra* note 6 (emphasizing importance of decision for journalists). Journalists are often the victims of monitoring and surveillance. *See id.* In 2019, a letter signed by 103 organizations was submitted to the U.S. Department of Homeland Security "rais[ed] concerns over reports of surveillance activities" involving journalists and reporters. *Id.* "The letter . . . warn[ed] that surveillance of journalists may violate the Privacy Act and infringe on the rights of the press." *Id.*

[56] *See id.* (recognizing "recent high-profile examples of government efforts to monitor journalists.")

[57] *See* Garris v. FBI, 937 F.3d 1284, 1296 (9th Cir. 2019) (explaining court will "consider the factors for and against the maintenance of such records of First Amendment activities on an individual, case-by-case basis."); *see also* MacPherson v. IRS, 803 F.2d 479, 484 (9th Cir. 1986) (declining to create bright line rule).

> [W]e decline to fashion a hard and fast standard for determining whether a record of First Amendment activity is exempt from section (e)(7) of the Privacy Act because it is "pertinent to and within the scope of an authorized law enforcement activity." The strong policy concerns on both sides of the issue present close and difficult questions and may balance differently in different cases. We therefore elect to consider the factors for and against the maintenance of such records of First Amendment activities on an individual, case-by-case basis.

MacPherson, 803 F.2d at 484.

[58] *See* Wajert, *supra* note 6 (noting importance of law enforcement activity exception despite being rarely considered); Becker, *Dossiers*, *supra* note 18, at 717 (explaining conflict among circuits). *But see* Lindblom v. FBI, 522 U.S. 913 (1997) (declining to hear case of *J. Roderick MacArthur Foundation v. FBI*). The Circuit for the District of Columbia held that law enforcement agencies are not required to expunge records of First Amendment activity when no longer pertinent to a current investigation. J. Roderick MacArthur Foundation v. FBI, 102 F.3d 600, 605 (D.C. Cir. 1996).

with the purpose of the Privacy Act, and in favor of protecting privacy rights, the Ninth Circuit held that a record had to be related to an ongoing, authorized law enforcement activity to be maintained. While some may argue against this decision, citing national security concerns, this holding does not eliminate the ability for the government to effectively do their job and instead merely emphasizes the importance of respecting constitutional rights. Overall, this decision is promising for citizens' privacy rights in a world shifting towards increased electronic communication in conjunction with constant technological advances that make surveillance too easy.

Megan Ryan