NO. 18-15416

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

DENNIS JOSEPH RAIMONDO, et al.,

PLAINTIFFS-APPELLANTS,

v.

FEDERAL BUREAU OF INVESTIGATION,

DEFENDANT-APPELLEE.

On Appeal from the U.S. District Court for Northern California
No. 3:13-cv-02295-JSC
The Honorable Jacqueline Scott Corley

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS-APPELLANTS

Aaron Mackey
Camille Fischer
Adam Schwartz
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: amackey@eff.org
Telephone: (415) 436-9333

Counsel for Amicus Curiae
Electronic Frontier Foundation

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *Amicus Curiae* Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes, Rules, and Regulations

Other Authorities

Legislative Authorities

STATEMENT OF INTEREST[1]

Amicus curiae Electronic Frontier Foundation (EFF) is a non-profit civil liberties organization with more than 40,000 members that works to protect rights in the digital world. Based in San Francisco and founded in 1990, EFF regularly advocates in courts and broader policy debates on behalf of users and creators of technology in support of free expression, privacy, and innovation.

As a recognized expert focusing on the intersection of civil liberties and technology, EFF is particularly concerned with protecting the constitutional rights to free speech and digital privacy at a time when technological advances have resulted in an increased ability of the government to pry into the private lives and expressive activities of innocent Americans. EFF frequently files Freedom of Information Act and Privacy Act requests and litigates them to learn more about federal law enforcement practices that target the speech and privacy interests of people in the United States.

[1] No party's counsel authored this brief in whole or in part. Neither any party nor any party's counsel contributed money that was intended to fund preparing or submitting this brief. No person other than *amicus*, its members, or its counsel contributed money that was intended to fund preparing or submitting this brief. The parties have consented to the filing of this brief.

INTRODUCTION

The Privacy Act places critical limits on federal government programs that collect and maintain personal records about people in the United States. 5 U.S.C. § 552a. Of greatest importance here, the Act bars the government from maintaining records of First Amendment activities, *Id.* at § 552a(e)(7), which protects the Constitutional rights to speak, associate, and think freely. The prescient fears of the Act's authors have been proven true by forty years of technological innovation that have given the federal government unprecedented ability to capture and stockpile data about the public's First Amendment activity. Unfortunately, by misinterpreting the Act's exception for "authorized law enforcement activity," the Federal Bureau of Investigation (FBI) and other federal law enforcement agencies erroneously assert a prerogative to retain any piece of information about First Amendment activity that could potentially have a future law enforcement use.

That is what happened to Mr. Raimondo and Mr. Garris. The FBI has collected and maintained records of their online activism and journalism since the early 2000s under the guise of a "threat assessment," which involves FBI surveillance of individuals and their online activity without judicial or administrative oversight. For speaking out against the Patriot Act and war in the Middle East—which is clearly protected by the First Amendment—the FBI surveilled them, and now maintains easily retrieved records about their speech.

The FBI activity at issue in this case is all too common. The rapid growth of the Internet has enabled billions of people to connect, collaborate, and express their views. But concentrating expressive activity online has also exponentially expanded law enforcement's surveillance capabilities. Now, after a quick search on the Internet, officers can find years of public online posts gathered across social media, online blogs, and even the comments sections of news stories. Further, a revolution in data management technology enables the FBI and other law enforcement agencies to inexpensively store, and instantaneously retrieve, oceans of sensitive information about people's First Amendment activities.

Although much of this speech may be on public webpages, law enforcement should not be allowed to maintain it in government files in perpetuity when the record is not relevant to an active investigation. That practice is contrary to the text and purpose of the Privacy Act. And when federal law enforcement does so, it chills speech and association in the "vast democratic forums of the Internet." *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017) (quoting *Reno v. ACLU*, 521 U.S. 844, 868 (1997)). This is particularly true for marginalized groups and those who voice unpopular or dissenting views.

Finally, the factors at issue in *MacPherson v. I.R.S.*, 803 F. 2d 479, 484-85 (9th Cir. 1986), which led the court to deny Privacy Act expungement, are not present in this case. Surveillance of the Internet, as here, is far more thorough and

far less labor-intensive than the monitoring of a political gathering by an undercover agent, as in *MacPherson*. And word searches of modern digital databases, as here, are far more likely to retrieve records of a speaker's First Amendment activity, compared to the more primitive record-keeping system in *MacPherson*, in which the information about the speaker was not indexed to their name.

ARGUMENT

I. THE PRIVACY ACT'S AUTHORS INTENDED IT TO PROVIDE STRONG PROTECTION FROM POLITICAL SPYING.

Congress enacted the Privacy Act in 1974, among other reasons, to constrain the executive branch from undertaking domestic surveillance of First Amendment activity. But in the modern era, through advanced computing technologies, it is all too easy for law enforcement to monitor Americans over the Internet and collect and retain information about them in perpetuity.

In the decades before the passage of the Privacy Act, the U.S. government ramped up its surveillance of opposing political viewpoints—most often minority speakers who had been marginalized and unfairly treated by U.S. policy. Through the domestic counterintelligence program COINTERLPRO, the FBI infamously tracked the Reverend Dr. Martin Luther King, Jr. and other members of the Southern Christian Leadership Conference—mislabeling them as "Black

Nationalist Hate Groups"—in an attempt to sabotage the Civil Rights Movement.[2] The U.S. Army deployed similar programs to "keep surveillance over the way the civilian population expressed [its] sentiments about government policies," including tracking the views expressed by students, clergy, and advocacy groups. S. Rep. No. 1183, 93d Cong., 2d Sess., *reprinted in* 1974 U.S. Code Cong. & Admin. News 6916, 6928.

When the U.S. House of Representatives considered the Privacy Act, the recent revelation that the President had ordered the FBI to conduct political espionage against the Democratic Party created an immediacy to enact new statutory safeguards to prevent such political spying in the future. Representatives cited the executive's actions as direct evidence of why the government should be prevented from surveilling First Amendment activity, such as the break-in of the Democratic National Committee's headquarters in June 1972, the revelation that the White House surveilled people on an "enemies list," the misuse of CIA files to silence the whistleblower who revealed the Pentagon Papers, the wiretapping of news reporters' conversations with government employees, and the taping of personal conversations in the Oval Office itself. *See* H.R. Rep. No. 1416, 93d Cong., 2d Sess., at 8-9 (1974).

[2] The Martin Luther King, Jr. Research and Education Institute, *Federal Bureau of Investigation (FBI)*, The Martin Luther King, Jr. Encyclopedia, https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi.

Responding to surveillance abuses of then-recent decades, Congress included in the Privacy Act the key provision at issue in this case—a prohibition against the government stockpiling records of how people exercise their rights to free speech and association. Specifically, the Act directs agencies to "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7). Given Congress' clear intent to reign in political spying, this rule's law enforcement exception must be read narrowly.

In light of the Act's legislative history, the Ninth Circuit has long expressed skepticism of "painting with such a broad stroke in this area of law." *MacPherson*, 803 F.2d at 483. Quoting this history, the court made clear: "The purpose of the section (e)(7) First Amendment protection is to prevent 'collection of protected information not immediately needed, about law-abiding Americans, on the off-chance that Government or the particular agency might possibly have to deal with them in the future.'" *Id*. (quoting S. Rep. 1183, U.S.C.C.A.N. 6916, 6971). The court then explained, in light of the legislative history and contemporaneous administrative guidelines, that the law enforcement exception must be read narrowly: "Congress did not intend to dilute the guarantees of the First

Amendment by authorizing the maintenance of files on 'persons who are merely exercising their constitutional rights.'" *Id.* (quoting *Clarkson v. IRS*, 678 F.2d 1368, 1374 (11th Cir. 1982)) (quoting OMB Guidelines, 40 Fed. Reg. 28965 (1975) (quoting floor debate in the Congressional record). Thus, the record established by Congress, as interpreted by the Ninth Circuit, shows that law enforcement bears a heavy burden to justify maintenance of records of First Amendment activity on grounds of an actual "authorized law enforcement purpose." 5 U.S.C. § 552a(e)(7).

II. THE FBI USES ASSESSMENTS TO COLLECT AND MAINTAIN RECORDS ABOUT THE FIRST AMENDMENT ACTIVITIES OF INNOCENT PEOPLE.

After the terrorist attacks on September 11, 2001, the FBI rapidly expanded its collection and maintenance of information about free speech and political expression, despite the Privacy Act's clear restraints on this maintenance.[3]

---

[3] In this brief, *amicus curiae* EFF addresses FBI rules in effect today: the *Attorney General's Guidelines* issued in 2008, and an FBI *Guide* issued in 2016. *See infra* notes 4 and 5. The language of these current FBI rules varies from the language of the FBI rules in effect when the FBI conducted its assessment of Mr. Raimondo and Mr. Garris. *See* U.S. Attorney General John Ashcroft, *The Attorney General's Guidelines on General Crimes,* Racketeering *Enterprise and Terrorism Enterprise Investigations* (May 30, 2002), https://epic.org/privacy/fbi/FBI-2002-Guidelines.pdf; U.S. Attorney General John Ashcroft, *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (Oct. 31, 2003), https://oig.justice.gov/special/0509/chapter5.htm#300. *See generally* Opening Brief of Appellants at 7-9, Dkt. No. 9 (filed July 27, 2018).

The FBI's current *Domestic Investigations and Operations Guide* has few restrictions on surveillance of First Amendment activity. Instead, it permits agents to "lawfully collect, retain, and consider the content of constitutionally protected speech, so long as: (i) the collection is logically related to an authorized investigative purpose; (ii) the collection does not actually infringe on the ability of the speaker to deliver his or her message; and (iii) the method of collection complies with the least intrusive method policy."[4] Under this *Guide*, FBI agents are free to collect and maintain records about First Amendment activity by searching the Internet.

"Assessments" are an FBI investigative process regulated by the U.S. Attorney General's *Guidelines for Domestic FBI Operations*.[5] To open an assessment, an FBI agent does not need "any particular factual predicate."[6] However, they do need an "authorized purpose," which includes obtaining information of "possible investigative interest" about "criminal or national

---

[4] FBI, *Domestic Investigations and Operations Guide* at Part 4.2.1 (Mar. 3, 2016), https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29%202016%20Version%20Part%2001%20of%2002/view.

[5] U.S. Attorney General Michael B. Mukasey, *The Attorney General's Guidelines for Domestic FBI Operations* (Sept. 29, 2008), https://www.justice.gov/archive/opa/docs/guidelines.pdf.

[6] *Id.* at 17.

security-threatening activities," including obtaining information about people who may be targeted by such activities.[7] In other words, agents may open an assessment based on a hunch and an "authorized purpose."

Further, FBI agents may open an assessment without any supervisory approval.[8] In carrying out an assessment, FBI agents are invited to "proactively surf[] the Internet to find publicly accessible websites and services . . ."[9] They are also encouraged to search existing FBI databases and other state and federal files for information about an assessment's target.[10]

Under the Attorney General's *Guidelines*, information gathered in an assessment is retained by the FBI, and available throughout the American intelligence and law enforcement communities.[11] Various FBI systems could facilitate dissemination of First Amendment information gathered during an assessment. For example, since at least 2012, the FBI has combined investigatory and intelligence files with publicly available information into a central data warehouse to "provide repositories where disparate data sets can be compared with each other and with FBI information to provide a more complete picture of

---

[7] *Id.* at 17.
[8] *Id.* at 18.
[9] *Id.* at 17. *See also id.* at 20 (authorizing agents to "use online services and resources").
[10] *Id.* at 20.
[11] *Id.* at 16.

potential national security threats or criminal activities."[12] Likewise, the FBI's automated case management system ensures that FBI-stored data can easily be searched and retrieved across its many field offices.[13]

FBI assessments are the lowest rung in the "different levels of information gathering activity" that agents may undertake.[14] When officers have "information indicative of possible criminal or national security-threatening activity," and supervisory approval, they may conduct "predicated investigations" (both "preliminary" and "full") using a broader set of investigatory techniques.[15] Given the intrusiveness of using the Internet to gather information about a target's First Amendment activity, *see infra* Part III, this technique should require supervisory review and a factual predicate, as in predicated investigations. But the Attorney General's *Guidelines* instead relegate this intrusive practice to unsupervised and unpredicated assessments. This is all the more reason to rigorously enforce the Privacy Act's ban on long-term maintenance of First Amendment information collected through web-surfing during an FBI assessment.

The assessment in this case highlights the invasive power of the technique.

---

[12] Privacy Act of 1974 System of Records Notice, 77 Fed. Reg. 40,630, 40,630 (July 10, 2012).

[13] FBI, *Privacy Impact Assessment for the SENTINEL System* (May 28, 2014), https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/sentinel.

[14] Mukasey, *The Attorney General's Guidelines*, *supra*, at 17.

[15] *Id.* at 18, 20.

Specifically, agents surfed the Internet, gathered information about Mr. Raimondo and Mr. Garris, and stored that information in the FBI's files. To this day, many years after the FBI ended its assessment of them without finding any misconduct or reason to elevate the assessment to an actual investigation, the FBI makes that information available to officials throughout the country. This lawsuit is about a critical check on this power: the Privacy Act's requirement that the FBI expunge information about First Amendment activities.

III. THE EXPLOSIVE GROWTH OF THE INTERNET, AND POLICE TECHNOLOGIES TO SCRUTINIZE THE INTERNET, HAS EXPANDED POLITICAL SPYING, CHILLED FIRST AMENDMENT ACTIVITY, AND DISPARATELY BURDENED MINORITY COMMUNITIES.

The technological revolution of the last generation has yielded the most important communications tool ever invented: the Internet. But ironically, it often is easier for law enforcement to monitor First Amendment activity on the Internet than anywhere else. Worse, police have developed surveillance tools and programs directed at political speech on the Internet. As with political spying throughout our nation's history, police scrutiny of First Amendment activity on the Internet chills and deters expression in this critical democratic forum, and leads to unfairly disparate snooping on the speech of minority communities and political dissidents. All of this requires robust application of the Privacy Act's expungement remedy when the FBI mines the Internet for First Amendment information.

A. Surveillance of First Amendment Activity on the Internet Vastly Increases the Harms of Political Spying Because it Creates a Detailed Picture of a Person's Views.

A generation ago, if FBI agents wanted to know what a target organization's members were saying, agents may have had to attend an organizational meeting, as agents did in *MacPherson*. *See* 803 F.2d at 480. Today, FBI agents can find far more information about what an organization is saying, with far less effort, by simply searching the Internet. This automation is a game changer: it means the FBI has the technological capacity to gather and store exponentially more information about First Amendment activity.

This change has constitutional significance. Earlier this year, the Supreme Court held that police access to detailed, historic records about an individual's location, even when collected by a third-party, "implicates privacy concerns far beyond those considered" in previous cases that involved police acquisition of business records that held far less information about customers, because they were collected by more primitive technologies than are used today. *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018). The Court held that acquisition of location records that show a person's movements over an extended period of time was a search requiring a warrant. *See id.* at 2209. The Court reasoned: "[T]his case is not about 'using a phone' or a person's movement at a particular time. It is about a

detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Id*. at 2220.

In *United States v. Jones*, a majority of the Justices of the Supreme Court likewise determined that longer-term GPS location surveillance impinges on reasonable expectations of privacy. *See* 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); *id.* at 412 (Alito, J., concurring in the judgment). These Justices distinguished contemporary GPS technology from more primitive "beeper" tracking tools. *Id.* at 417 n.*; *id.* at 429 n.10. As Justice Sotomayor explained:

> [T]he Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring – by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track – may alter the relationship between citizen and government in a way that is inimical to a democratic society.

Id. at 416 (internal quotation removed).

Here, when FBI agents search the Internet for what a target or organization is saying, they can likewise obtain a detailed record over many years, which "implicates privacy concerns far beyond those" of the FBI's older surveillance methods. *Carpenter*, 138 S. Ct. at 2220.

This technological distinction also informs FOIA cases addressing privacy interests. For example, the Supreme Court upheld an agency's withholding of a person's "rap sheet," *i.e.*, a "computerized summary" of their arrest information,

even though the requester could have obtained the same information "after a diligent search of courthouse files, county archives, and local police stations throughout the country." *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 762-64 (1989). The Court reasoned that "compilation of otherwise hard-to-obtain information alters the privacy interest implicated." *Id.* at 764. Likewise, the ease here of using the Internet to gather and store First Amendment information vastly increases the harm from the FBI's violation of the Privacy Act.

B. New Automated Tools Make It Increasingly Easy For Law Enforcement to Collect, Store, and Share First Amendment Activity Located on the Internet.

The "vast democratic forums of the Internet," and "social media in particular," might be the "most important places . . . for the exchange of views." *Packingham*, 137 S.Ct. at 1735. But their accessibility also provides law enforcement an opportunity to monitor political communities with unprecedented ease and efficiency. This is especially hazardous when police use automated technologies to scour the Internet for First Amendment activity. The Privacy Act's ban on government retention of records about First Amendment activity is needed now more than ever, to ensure these new law enforcement powers do not degrade these critical digital forums.

For example, police can use computerized tools to automatically monitor First Amendment activity on social media. In 2016, the ACLU of Northern California revealed that law enforcement agencies had purchased access to a service called Geofeedia that exploited developer features within Facebook, Twitter, and Instagram to collect public posts.[16] This enabled law enforcement to not only search for a specific person's social media communications, but also to monitor speech trends, which police departments in Oakland[17] and Baltimore[18] have admitted to doing in order to keep tabs on protests against police brutality. After the ACLU's reporting, social media companies blocked Geofeedia's ability to collect public posts, but other tools will continue to arise to provide law enforcement detailed reports of online speech.

Likewise, a growing federal social media surveillance program targets foreign visitors, and, consequently, the many Americans who communicate with these visitors. Earlier this year, the federal government announced it will expressly

---

[16] Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU Northern California (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

[17] Ali Winston, *Oakland Cops Quietly Acquired Social Media Surveillance Tool*, East Bay Express (Apr. 13, 2016), https://www.eastbayexpress.com/oakland/oakland-cops-quietly-acquired-social-media-surveillance-tool/Content?oid=4747526.

[18] Geofeedia, *Case Study: Baltimore County PD,* https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

ask all foreign visitors for their social media account names when determining their eligibility to enter the United States.[19] An integrated social media "extreme vetting" program will harvest, preserve, and scrutinize immigrants' social media information.[20] The captured information will be stored in an immigrant's A-file, which contains the complete immigration and travel records of all VISA applicants, asylum seekers, lawful permanent residents, and even naturalized citizens. Internal government reports question the effectiveness of the program.[21] Even though the government has abandoned for now its ill-conceived plans to use computer algorithms to mine this data and determine which visitors are most likely to be violent,[22] constant vigilance is needed to prevent the adoption of future

---

[19] Sophia Cope and Adam Schwartz, *DHS Should Stop the Social Media Surveillance of Immigrants*, EFF Deeplinks Blog (Oct. 3, 2017), https://www.eff.org/deeplinks/2017/10/dhs-should-stop-social-media-surveillance-immigrants.

[20] Aleksander Danielyan, *EFF Urges DHS to Abandon Social Media Surveillance and Automated "Extreme Vetting" of Immigrants*, EFF Deeplinks Blog (Nov. 16, 2017), https://www.eff.org/deeplinks/2017/11/eff-urges-dhs-abandon-social-media-surveillance-and-automated-extreme-vetting.

[21] Manar Waheed, *New Documents Underscore Problems of 'Social Media Vetting' of Immigrants,* ACLU (Jan. 3, 2018), https://www.aclu.org/blog/privacy-technology/internet-privacy/new-documents-underscore-problems-social-media-vetting.

[22] Drew Harwell and Nick Miroff, *ICE just abandoned its dream of extreme vetting software that could predict whether a foreign visitor would become a terrorist*, Washington Post (May 17, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/?utm_term=.40cb6aaa3361.

iterations of this dangerous plan. While this "extreme vetting" program ostensibly targets foreign visitors, it will inevitably sweep up the many Americans who use social media to communicate with these foreigners—and these Americans are disproportionately immigrants and people of color.

Advanced computing technologies also make it far more efficient for law enforcement agencies to share with each other the large volumes of sensitive personal data that they mine and warehouse. For example, the Department of Homeland Security (DHS) recently announced its intention to build a new database, called Homeland Advanced Recognition Technology (HART), that creates complex biometric and biographic profiles of persons using data from a multitude of sources, including FBI databases.[23] This will include biometric data, often collected in dubious circumstances, and often riddled with error.[24] Most significantly for current purposes, HART will contain "records related to the analysis of relationship patterns about individuals," including "non-obvious relationships."[25] This will inevitably intrude upon the First Amendment right to

[23] Jennifer Lynch, *HART: Homeland Security's Massive New Database Will Include Facial Recognition and Peoples' 'Non-Obvious Relationships*, EFF Deeplinks Blog (June 7, 2018), https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and.
[24] *Id*.
[25] *Id*.

privacy in expressive associations. *See, e.g., NAACP v. Alabama*, 357 U.S. 449 (1958).

To meet the many new challenges posed by rapidly-improving technologies that amplify the powers of police to gather, store, and share information about First Amendment activity on the Internet, courts must scrupulously enforce the Privacy Act's ban on maintenance of records about such activity.

C. Government Surveillance Programs Chill the Exercise of First Amendment Rights.

Law enforcement causes serious social harm by indefinitely keeping records of First Amendment activity, especially in cases (as here) where such records are not relevant to current investigations.

In interpreting this exception to the Privacy Act, this Court has long acknowledged the harm to individual speech caused by law enforcement surveillance programs: "We recognize that even 'incidental' surveillance and recording of innocent people exercising their First Amendment rights may have a 'chilling effect' on those rights that section (e)(7) [of the Privacy Act] was intended to prohibit. 'The mere compilation by the government of records describing the exercise of First Amendment freedoms creates the possibility that those records will be used to the speaker's detriment and hence has a chilling effect on such exercise.'" *MacPherson*, 803 F.2d at 484 (quoting *Nagel v. U.S. Dep't of Health, Education, and Welfare*, 725 F.2d. 1438, 1441 (D.C. Cir. 1984)).

This chilling effect is well documented by decades of sociological research. In 1974, the same year the Privacy Act was passed, political scientist Elizabeth Noelle-Neumann identified a "spiral of silence," in which people continuously monitor their environments to determine whether they hold the minority point of view, and adjust their speech based on whether the majority is hostile to their viewpoint.[26] A recent study examining the "spiral of silence" in the context of the disclosure of controversial mass surveillance programs conducted by the U.S. National Security Agency (NSA) has further shown that government surveillance chills minority viewpoints and reinforces the majority viewpoint.[27]

Likewise, the Pew Research Center in 2014 studied the chill on speech that followed the disclosure of the NSA's domestic spying program, and found that 87% of Americans "are aware that their online actions are subject to government interception, a higher percentage than those who can identify the federal minimum wage."[28] The Center also found variation in where respondents were willing to discuss the NSA's surveillance programs: less than half of respondents would

---

[26] Elizabeth Noelle-Neumann, *The spiral of silence: Public opinion—Our social skin* (Univ. of Chicago Press 2d ed. 1993).

[27] Elizabeth Stoychef, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in Wake of NSA Internet Monitoring*, Journalism of Mass Comm. Q. (Mar. 8, 2016), http://journals.sagepub.com/doi/10.1177/1077699016630255.

[28] *Id*.

discuss the programs online, where the government might be listening, compared to 86% who were willing to discuss it in-person.[29]

In 2013, EFF filed a lawsuit in the U.S. District Court for Northern California on behalf of an ideologically diverse array of clients, alleging their speech and the speech of their members had been chilled by the NSA's mass surveillance of all domestic telephone metadata (*e.g.*, records of who calls whom and when).[30] Plaintiffs' declarations describe in detail how this surveillance chills speech and association. Many clients of Human Rights Watch refrained from contacting them to receive help responding to government abuse, out of fear that the NSA might track their call metadata.[31] The Shalom Center delayed publication of academic articles criticizing U.S. policy in Syria, out of fear it would draw the NSA's attention.[32] The Center's Director had previously been subjected by the FBI to COINTELPRO surveillance, and thus he had additional fear of NSA surveillance. And the Council for American-Islamic Relations faced serious difficulties in communicating with their clients, who were afraid to discuss the

---

[29] Pew Research Center, *From ISIS to unemployment: What do Americans know?* (Oct. 2, 2014), http://www.people-press.org/2014/10/02/from-isis-to-unemployment-what-do-americans-know/.

[30] *See* Complaint, *First Unitarian Church of L.A. v. NSA,* https://www.eff.org/node/75009.

[31] *See* Decl. of Human Rights Watch, *First Unitarian Church of L.A. v. NSA*, https://www.eff.org/document/human-rights-watch.

[32] *See* Decl. of Shalom Center, *First Unitarian Church of L.A. v. NSA*, https://www.eff.org/document/shalom-center-declaration.

sensitive details of their cases by phone or email, under the assumption that the federal government was monitoring their speech because of their religion.[33]

D. Police Actively Use Internet-Based Surveillance Technologies to Track Minority and Dissident Voices.

If courts allow the law enforcement community to evade the clear limits of the Privacy Act, and to amass and share ever-growing dossiers about how Americans exercise their First Amendment rights to speak and associate on the Internet, it is highly likely that the victims will disproportionately include people of color and political dissidents.

Since 9/11, the FBI has increased its warrantless tracking of so-called "suspicious" persons. For example, the FBI's eGuardian program, created in 2007, centralizes "Suspicious Activities Reporting" so local law enforcement can share information on supposedly "suspicious persons" directly with the federal government and with peer jurisdictions.[34] Law enforcement is encouraged to collect information about anything that appears to have a "potential nexus to terrorism," and data can be kept for five years for trend analysis.[35] Items reported to eGuardian often target people in the U.S. based on their religious and ethnic

---

[33] *See* Decl. for the Council on American Islamic Relations, *First Unitarian Church of L.A. v. NSA*, https://www.eff.org/document/cair-declaration.

[34] FBI, *eGaurdian*, Resources: Law Enforcement, https://www.fbi.gov/resources/law-enforcement/eguardian.

[35] FBI, *Privacy Impact Assessment for the eGuardian System* (Jan. 4, 2013), https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/eguardian-threat.

identities, like reports of "a substantial increase in the presence of female Muslims fully dressed in veils/burkas," or a "suspicious gathering" of Middle Eastern-looking people.[36] When briefed about the program, many local law enforcement agencies had serious privacy and First Amendment concerns, and many determined that they would not share information with the FBI that they had not first personally vetted as a credible threat.[37]

In the last few years, the FBI has also surveilled civil rights activists who advocate for the end to police shootings that have killed thousands of African American men and women.[38] One FBI report documents the agency's scrutiny of a Black Lives Matter (BLM) activist's innocent First Amendment activity: flying from New York to protests in Ferguson, Missouri, and raising money to post bail for arrested protesters.[39] The report also shows that local police asked the FBI to

---

[36] Ryan J. Reilly, *FBI's eGuargian Program For Reporting Suspicious Activity Raised Civil Rights Concerns*, HuffPost (Oct. 30, 2013), https://www.huffingtonpost.com/2013/10/30/eguardian-fbi-suspicious-activity-reporting_n_4178272.html.

[37] Nusrat Choudhury, *Where's the Suspicion in Government's 'Suspicious Activity' Reports?*, ACLU (Oct. 30, 2013), https://www.aclu.org/blog/national-security/wheres-suspicion-governments-suspicious-activity-reports.

[38] George Joseph and Murtaza Hussain, *FBI Tracked an Activist Involved with Black Lives Matter as they Traveled Across the US; Documents Show*, The Intercept (Mar. 19, 2018), https://theintercept.com/2018/03/19/black-lives-matter-fbi-surveillance/.

[39] FBI Report (Nov. 21, 2014), https://www.documentcloud.org/documents/4412917-FBI-Intelligence-Report-Tracking-Black-Lives.html.

look into this person in connection with the Ferguson protests, and that the FBI searched their internal databases but returned no responsive records about the activist. Another FBI report shows that agents "staked out" BLM activists' cars and residences to track their movements, and talked to "confidential human sources" about the activists.[40]

The FBI has sought to legitimize such unjustified political spying by inventing from whole cloth an otherwise non-existent movement in supposed need of police monitoring: "Black Identity Extremists."[41] One law enforcement training document dubiously defines this moniker as "domestic terror groups and criminally subversive subcultures which are encountered by law enforcement professionals on a daily basis."[42] The FBI's own Intelligence Assessment of "Black Identity Extremists" states: "The FBI assesses it is very likely that BIEs' perception of unjust treatment of African Americans and the perceived

---

[40] FBI Report (Nov. 25, 2014), https://www.documentcloud.org/documents/4412923-FBI-Intelligence-Report-on-Surveillance-of-Cars.html.

[41] Jana Winter and Sharon Weinberger, *The FBI's New U.S. Terrorist Threat 'Black Identity Extremists'*, Foreign Policy (Oct. 6, 2017), https://foreignpolicy.com/2017/10/06/the-fbi-has-identified-a-new-domestic-terrorist-threat-and-its-black-identity-extremists/.

[42] Virginia Dept. of Criminal Justice Services, *Introduction to Domestic Extremism and Hate Groups*, Law Enforcement Training Course (Sept. 5, 2018), https://www.dcjs.virginia.gov/training-events/introduction-domestic-extremism-and-hate-groups.

unchallenged illegitimate actions of law enforcement will inspire premeditated attacks against law enforcement over the next year."[43]

In short, FBI agents in too many circumstances are insufficiently restrained in conducting surveillance against minority and opposition voices. Worse, the high tech efficiencies created by the Internet and modern computing vastly amplify the harmful consequences of this political spying. As FBI assessments and other forms of suspicionless surveillance increase, it is imperative for courts to uphold the accountability mechanisms of the Privacy Act, including file expungement.

IV. THIS COURT SHOULD INTERPRET THE PRIVACY ACT TO ACCOUNT FOR ADVANCES IN TECHNOLOGY SINCE 1986, WHEN IT DECIDED *MACPHERSON*.

The mechanisms and prevalence of government surveillance have radically changed since 1986, when this Court in *MacPherson* last addressed expungement under the Privacy Act. Today, this Court should apply *MacPherson* in light of this technological transformation, and consistently with the protective intentions of the authors of the Privacy Act. The Act's ban on maintaining information about First Amendment activity creates a critical failsafe against political spying. So it is imperative that this Court limit the Privacy Act's law enforcement exception to

[43] FBI Intelligence Assessment, *Black Identity Extremists Likely Motivated to Target Law Enforcement Officers*, (Aug. 3, 2017), https://www.documentcloud.org/documents/4067711-BIE-Redacted.html.

First Amendment activity that the FBI currently needs to conduct an active investigation.

In *MacPherson*, this Court held that Privacy Act expungement requests should be analyzed by "on an individual, case-by-case basis." 803 F.2d at 484. When this Court ruled that the IRS could keep its records of Mr. MacPherson's public anti-tax speeches, it did so principally because (1) Mr. McPherson made and sold his convention speeches to the general public, including an undercover IRS agent, and (2) the IRS retained records of that speech not to track Mr. MacPherson, but rather to provide context around the larger anti-tax movement. *Id*. This Court also emphasized the facts that the IRS had to purchase the tapes, and that the files were only physically shared between two IRS offices. *Id*. The case at bar is fundamentally different.

A. Changes In Collection from *MacPherson* to *Raimondo*.

FBI threat assessments based on Internet activity, including the assessment conducted against Mr. Raimondo and Mr. Garris, are a completely different paradigm of government surveillance, compared to IRS monitoring of a tax protester conference. The way people communicate about political issues has fundamentally changed with the adoption of email, online blogging, and social media. The Supreme Court has recognized that social media is the "most important place" for the exchange of ideas. *Packingham*, 137, S. Ct. at 1735. Rather than the

labor-intensive process of attending a conference, and taking notes about a speech that may be of interest to law enforcement, agents can now stay in their offices to monitor people all over the country with a click of the mouse. Further, such surveillance can be far more thorough. For example, if agents see a public post on a website like Twitter, and then click on a person's name, officers can quickly and easily download years of ideas and speech.

In the past, when agents had to be physically present to surveil speech, they had to justify the use of scarce time and resources to monitor a target. Now, because such large quantities of speech can be collected from publicly available information online, and because law enforcement has access to computerized systems with billions of records about the public, agents can surveil people far more easily.

Thus, while the public nature of Mr. MacPherson's expression at a tax protest conference weighed against his Privacy Act expungement claim, the same is not true for the public nature of Mr. Raimondo's and Mr. Garris' expression on a political website. This is because the 20th century snooping techniques in *MacPherson* were labor-intensive and episodic, while the 21st century snooping techniques in *Raimondo* were automated and systematic. This technological transformation makes a critical constitutional difference. *See, e.g., Carpenter* and *Jones, supra.*

B. Changes in Storage and Sharing from *MacPherson* to *Raimondo*.

Of equal importance, technological innovation in the last 30 years has fundamentally transformed the way that government agencies maintain and share their files. In *MacPherson*, the IRS stored its information about Mr. MacPherson's First Amendment activity in a file indexed to the anti-tax movement, and not indexed to Mr. MacPherson himself. 803 F.2d at 485 n.9. As a result, there was a greatly diminished possibility that any subsequent law enforcement scrutiny of Mr. MacPherson would uncover this record about his anti-tax speech. As the court emphasized, the files were not "filed under his name." *Id.* But today, law enforcement record-keeping is far different. For example, word searches of databases can uncover a record that contains a target's name, regardless of whether the target's name appears in the record's title or the database's index.

Moreover, as exemplified by the FBI databases and record keeping practices discussed above, there is a growing trend in law enforcement record sharing across federal agencies, and between local governments and federal agencies. These databases also allow information collected from completely different law enforcement programs to be searched simultaneously in other databases through the use of keywords.

Opponents of a robust Privacy Act expungement remedy have objected that it might impose administrative burdens on law enforcement agencies. *See, e.g., J.*

Roderick MacArthur Foundation v. FBI, 102 F. 3d 600, 604 (D.C. Cir. 1996). But the modernization of government databases greatly increases the efficiencies in responding to the public's Privacy Act expungement requests. While compliance in the past may have posed some burden in searching FBI field offices, *id.,* the integrated databases and case management systems used by the FBI today would greatly reduce the time it would take to find and delete records.

Finally, the growing size and accessibility of law enforcement databases have created new opportunities for government officials to abuse these databases for their own personal gain. In 2013, an internal NSA investigation determined that at least a dozen NSA employees used surveillance tools to spy on their former spouses and lovers.[44] Likewise, California police officers have used an expansive California police database to stalk their ex-partners,[45] gain advantage in custody proceedings,[46] and screen potential online dates.[47] Expungement is the best way to

---

[44] Alina Selyukh, *NSA staff used spy tolls on spouses, ex-lovers: watchdog*, Reuters (Sept. 27, 2013), https://www.reuters.com/article/us-usa-surveillance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927?feedType=RSS&feedName=domesticNews.

[45] Dave Maass, *California Authorities Are Failing to Track and Prevent Abuse of Police Databases*, EFF Deeplinks Blog (May 14, 2017), https://www.eff.org/deeplinks/2017/05/california-authorities-still-ignoring-rising-abuse-police-databases.

[46] David Minsky, *Down in the database dumps: Lawsuit highlights concerns for database misuse within California law enforcement*, Santa Maria Sun News (Dec. 10, 2016), http://www.santamariasun.com/news/13961/down-in-the-database-

ensure that government employees do not have the opportunity to abuse law enforcement records of the First Amendment activity of innocent people.

Accordingly, in light of transformative technological developments that vastly expand the government's power to store and share sensitive First Amendment information, the Privacy Act must be interpreted to curtail the maintenance of such information that is not relevant to a current investigation.

CONCLUSION

Amicus curiae EFF respectfully urges this Court to rule that under the Privacy Act, the FBI must expunge the assessment it retains on Mr. Raimondo and Mr. Garris.

Dated: August 3, 2018

Respectfully Submitted,

/s/ Aaron Mackey

Aaron Mackey
Camille Fischer
Adam Schwartz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
amackey@eff.org

Counsel for Amicus Curiae Electronic Frontier Foundation

---

dumps-lawsuit-highlights-concerns-for-database-misuse-within-california-law-enforcement-/.

[47] LA District Attorney Declination Letter, (May 14, 2012), https://www.eff.org/document/la-district-attorney-declination-letter-morales.

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(A)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amici Curiae Electronic Frontier Foundation In Support of Plaintiffs-Appellants complies with the type-volume limitation, because this brief contains 6,147 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: August 7, 2018

/s/ Aaron Mackey
Aaron Mackey

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on August 3, 2018.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: August 3, 2018

/s/ Aaron Mackey
Aaron Mackey

Counsel for Amicus Curiae
Electronic Frontier Foundation