

14-42

IN THE
United States Court of Appeals
FOR THE
Second Circuit

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES UNION FOUNDATION; NEW YORK CIVIL LIBERTIES UNION; and NEW YORK CIVIL LIBERTIES UNION FOUNDATION,

Plaintiffs-Appellants,

— v. —

JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; KEITH B. ALEXANDER, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; CHARLES T. HAGEL, in his official capacity as Secretary of Defense; ERIC H. HOLDER, in his official capacity as Attorney General of the United States; and ROBERT S. MUELLER III, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF OF *AMICUS CURIAE*
NATIONAL RIFLE ASSOCIATION OF AMERICA, INC.
IN SUPPORT OF PLAINTIFFS-APPELLANTS,
AND SUPPORTING REVERSAL

John Frazer
Law Office of John Frazer, PLLC
3925 Chain Bridge Road, Suite 403
Fairfax, VA 22030
Phone: (703) 352-7276
jfrazier@ifrazierlaw.com

RULE 29 CORPORATE DISCLOSURE STATEMENT

Amicus curiae is a non-profit membership corporation. It has no stock and no parent corporation. No corporation owns more than 10% of its stock.

TABLE OF CONTENTS

	<u>Page</u>
TABLE OF AUTHORITIES	v
INTEREST OF <i>AMICUS CURIAE</i>	1
SUMMARY OF ARGUMENT	4
ARGUMENT	5
I. The mass surveillance program threatens the First Amendment rights of the NRA and its members.	5
A. The mass surveillance program could allow identification of NRA members, supporters, potential members, and other persons with whom the NRA communicates, potentially chilling their willingness to communicate with the NRA.....	6
B. Modern data analysis techniques, and the risk of public disclosure, heighten First Amendment concerns about the mass surveillance program.	12
II. The mass surveillance program could allow the government to circumvent legal protections for Americans’ privacy, such as laws that guard against the registration of guns or gun owners.	15
A. The government’s interpretation of Section 215 would nullify statutory protections against centralization of gun ownership records.	19
B. The government’s interpretation of Section 215 conflicts with contemporaneously enacted protections for gun owners’ privacy.....	23
C. The government’s interpretation of Section 215, coupled with the potential gathering and aggregation of other forms of data, could allow	

the easy identification of gun owners, contrary to all privacy protections enacted by Congress.....	26
CONCLUSION.....	28

TABLE OF AUTHORITIES

<u>Cases</u>	<u>Page</u>
<i>Buckley v. Valeo</i> , 424 U.S. 1 (1976).....	7
<i>Doe v. Reed</i> , 130 S. Ct. 2811 (2010)	13
<i>Gibson v. Florida Legislative Investigation Comm.</i> , 372 U.S. 539 (1963).....	6
<i>McConnell v. Federal Election Comm’n</i> , 540 U.S. 93 (2003).....	8
<i>McIntyre v. Ohio</i> , 514 U.S. 334 (1995)	7
<i>Nat’l Shooting Sports Found., Inc. v. Jones</i> , 716 F.3d 200 (D.C. Cir. 2013)	21
<i>Nat’l Ass’n for Advancement of Colored People v. State of Ala. ex rel. Patterson</i> , 357 U.S. 449 (1958).....	4, 6-7
<i>Nat’l Rifle Ass’n v. Federal Election Comm’n</i> (Nos. 02-0581/02-0581) (D.D.C. 2002).....	9
<i>Pullen v. Morgenthau</i> , 73 F.2d 281 (2d Cir. 1934)	18
<i>RSM, Inc. v. Buckles</i> , 254 F.3d 61 (4th Cir. 2001).....	22
<i>Rumsfeld v. Forum for Academic & Institutional Rights, Inc.</i> , 547 U.S. 47 (2006).....	7
<i>S.E.C. v. Rosenthal</i> , 650 F.3d 156 (2d Cir. 2011)	17
<i>United States v. Jones</i> , 132 S. Ct. 945, 957, 181 L. Ed. 2d 911 (2012).....	10
 <u>Constitutional Materials and Statutes</u>	
13 U.S.C. § 9, 214.....	18
18 U.S.C. § 922(t)(2)(C).....	21

18 U.S.C. § 923(g)..... 20

18 U.S.C. § 923(g)(4) 24

18 U.S.C. § 926(a) 20, 22

50 U.S.C. § 1861.....4

50 U.S.C. § 1861(a)(2)..... 22

50 U.S.C. § 1862.....4

45 C.F.R. § 164.530(c) (2011)..... 15

Firearms Regulations, 43 Fed. Reg. 11,800 (Mar. 21, 1978)..... 23

National Instant Criminal Background Check System Regulation,
64 Fed. Reg. 10260-02 (March 3, 1999) 25

114 Cong. Rec. H22267 (daily ed. July 19, 1968) 19

114 Cong. Rec. S27420-421 (daily ed. Sept. 18, 1968) 19

131 Cong. Rec. S9163-64 (July 9, 1985)..... 20

An Act making appropriations for the Treasury Dep’t, the United States
Postal Serv., the Executive Office of the President, and certain Indep.
Agencies, for the fiscal year ending Sept. 30, 1979, and for other
purposes. Pub. L. No. 95–429, 92 Stat 1001 (Oct. 10, 1978)..... 23-24

Anti-Terrorism and Effective Death Penalty Act of 1996,
Pub. L. 104-132, 110 Stat. 1214 (Apr. 24, 1996).....3

Brady Handgun Violence Prevention Act of 1993, Pub. L. No. 103–159, 107
Stat. 1536 (Nov. 30, 1993) 20-21

Consolidated and Further Continuing Appropriations Act, 2012, Pub. L. No.
112-55, 125 Stat. 552 (Nov. 18, 2011) 24-26

Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, § 644,
117 Stat. 11,473-74 (Feb. 20, 2003)..... 25

Financial Services Modernization Act, 113 Stat. 1338 (1999) 15

Firearms Owners’ Protection Act of 1986, Pub. L. No. 99-308,
100 Stat. 449 (May 19, 1986)..... 20

Gun Control Act of 1968, Pub.L. 90-618, Title I, 82 Stat. 1213 (1968).....19

H. Amdt. 950 to H.R. 2703, 104th Cong. (1996).....3

Homeland Security Act of 2002, Pub. L. 107–296, 116 Stat 2135,
§ 1111(b) (2002).....23

Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272,
§ 602, 112 Stat. 2396, 2410-11 (1998).....4

Omnibus Consolidated and Emergency Supplemental Appropriations Act,
1999, Pub. L. No. 105–277, § 621, 112 Stat 2681 (October 21, 1998)... 25

Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, Title
IV, 82 Stat. 197, 225 (1968).....19

PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, § 2(a),
125 Stat.....24

USA PATRIOT Act, Pub. L. 107-56, § 215, 115 Stat. 272, 287-88 (2001)...4

Other

Marc Ambinder, *WikiLeaks: One Analyst, So Many Documents*, National
Journal, Nov. 29, 2010..... 14

Edward H. Baker, *How the NRA Sets the Standard for Customer
Engagement*, strategy+business, Dec. 19, 2013 available at
[http://www.strategy-business.com/blog/How-the-NRA-and-Apple-Set-
the-Standard-for-Customer-Engagement-A-QA-with-Peter-
Murray?gko=ba413](http://www.strategy-business.com/blog/How-the-NRA-and-Apple-Set-the-Standard-for-Customer-Engagement-A-QA-with-Peter-Murray?gko=ba413) (last viewed March 12, 2014)5

David I. Caplan, *Firearms Registration And Waiting Periods: New York City's Lesson*, *American Rifleman*, Oct. 1993 16

Edmund DeMarche, *NYPD cracks down on long guns that hold more than five rounds*, *FoxNews.com*, Dec. 5, 2013 available at <http://www.foxnews.com/us/2013/12/05/nypd-targets-owners-multi-clip-shotguns-rifles/> (last viewed March 12, 2014).....16

Victor Fiorillo, *These Philadelphians Want Gun Permits*, Philadelphia, Aug. 15, 2012, available at <http://www.phillymag.com/news/2012/08/15/philadelphia-gun-permit-appeals-reasons/> (last viewed March 12, 2014).....17

Brian Fung, *The NSA is giving your phone records to the DEA. And the DEA is covering it up.*, *The Washington Post*, Aug. 5, 2013, available at <http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/05/the-nsa-is-giving-your-phone-records-to-the-dea-and-the-dea-is-covering-it-up/> (last viewed March 12, 2014).....18

Barton Gellman, *NSA broke privacy rules thousands of times per year, audit finds*, *Washington Post*, Aug. 15, 2013 14

Barton Gellman and Ashkan Soltani, *NSA tracking cellphone locations worldwide, Snowden documents show*, *Washington Post*, Dec. 4, 2013.....10

Siobhan Gorman, *NSA Officers Spy on Love Interests*, *Wall Street Journal*, Aug. 23, 2013 14

Glenn Greenwald, *et al.*, *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, *The Guardian*, June 9, 2013 14

Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'*, *The Guardian*, July 31, 2013 10, 27

Jeff Johnston, *NRA's New Generation of Freedom Fighters*, *American Rifleman*, June 2003.....2

David Kopel, *Who Needs Guns? Lessons From Down Under*, *Chronicles*, Oct. 2003..... 16

Lessons Learned in Database Incident, Roanoke Times & World News, Mar. 25, 2007 17

Letter from Ronald Weich to Sens. Dianne Feinstein and Saxby Chambliss, Feb. 2, 2011, *available at* http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf (last visited Sept. 4, 2013)..... 10

Eric Lichtblau and Michael S. Schmidt, *Other Agencies Clamor for Data N.S.A. Compiles*, New York Times, Aug. 3, 2013.....18

C.B. Lister, *Firearms Laws in the 73d Congress*, American Rifleman, July 19345

Leona Mynes, *National Rifle Association Certifies Firearms Instructors*, U.S. Navy press release, May 5, 2010 *available at* http://www.navy.mil/submit/display.asp?story_id=53179 (last visited March 7, 2014).....2

Ellen Nakashima, *With better sharing of data comes danger*, Washington Post, Nov. 29, 2010..... 14

NRA Bylaws art. II..... 1

NRA Disavows Connections With Groups Advocating Violence, American Rifleman, Oct. 1964.....3

NRA Institute for Legislative Action, *Case against Wilmington Housing Authority Moves to State Supreme Court*, 2014 *available at* <http://www.nraila.org/legal/articles/2014/case-against-wilmington-housing-authority-moves-to-state-supreme-court.aspx> (last viewed March 10, 2014).....11, 12

Obama’s Remarks After Senate Gun Votes, The New York Times, April 17, 20137

Timothy O'Connor and Meghan E. Murphy, *Journal News gun permit map used by burglars to target White Plains home?*, Newsday, Jan. 13, 2013.....16

Policy Statement of the National Rifle Association on Extremist Organizations and Militia Groups, May 23, 1995.....3

Josh Richman, *Netroots Nation Features a Call to Action on Gun Control*, The Oakland Tribune, June 21, 2013 8

James Risen and Eric Lichtblau, *How the U.S. Uses Technology to Mine More Data More Quickly*, The New York Times, June 8, 2013..... 13

Jim Rutenberg, *Data You Can Believe In*, The New York Times, June 23, 2013 13

Michael D. Shear, *White House Denounces Web Video by N.R.A.*, The New York Times, January 16, 2013..... 8-9

Natasha Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, The New York Times, June 16, 2012 13

Christopher Swindell, *Gun safety debate is B.S.*, The Charleston Gazette, May 30, 20138

Terrorism Bill and Anti-Gun Exploiters, American Rifleman, Aug. 1995....3

Martha C. White, *Big Brother Is Watching You Swipe: The NSA’s Credit Card Data Grab*, Time, June 11, 2013..... 27

INTEREST OF *AMICUS CURIAE*

The National Rifle Association is a New York not-for-profit corporation.¹ All parties have consented to the filing of this brief.

The NRA believes that its participation as *amicus curiae* will materially aid the Court in resolving this case. The NRA represents millions of Americans who are concerned with simultaneously protecting national security, public safety, personal privacy, and the right to free speech. As a result, the NRA has a long history of advocacy directly related to key issues in this case.

First among the “Purposes and Objectives” listed in the NRA’s Bylaws is “[t]o protect and defend the Constitution of the United States,” and especially the right to keep and bear arms guaranteed by the Constitution. NRA Bylaws art. II. The NRA’s activities in support of that purpose have long included legislative advocacy and litigation concerning two issues relevant to this case: (1) the rights of the NRA and its members to associate and communicate freely under the First Amendment, and (2) the protection of gun owners against intrusive government surveillance or

¹ No party’s counsel authored this brief in whole or in part. No party or party’s counsel contributed money that was intended to fund preparing or submitting this brief. No person other than the *amicus curiae* contributed money that was intended to fund preparing or submitting this brief. *See* Second Circuit Local Rule 29.1.

recordkeeping, such as the establishment of systems to register or compile lists of firearms or the owners of firearms. The NRA's history of involvement in these issues—including direct lobbying on predecessor language to the statute at issue in this case—allows the NRA to offer a unique perspective in support of Appellants.

The NRA also stands second to no organization in its support for legitimate law enforcement, military, and national security activities to defend our nation against terrorism. Countless NRA members, including NRA employees, have served overseas in that fight since 2001. *See* Jeff Johnston, *NRA's New Generation of Freedom Fighters*, *American Rifleman*, June 2003, at 47. Indeed, the NRA was originally formed to promote improved military training, and today, the “Purposes and Objectives” described in the NRA's bylaws include the goals of “promot[ing] public safety, law and order, and the national defense,” as well as “train[ing] members of law enforcement agencies [and] the armed forces ... in marksmanship and in the safe handling and efficient use of small arms.” NRA Bylaws art. II. Those receiving such training in recent years have included military and security personnel at Naval Station Guantanamo Bay, Cuba. *See* Leona Mynes, *National Rifle Association Certifies Firearms Instructors*, U.S. Navy press release, May 5, 2010, *available at*

http://www.navy.mil/submit/display.asp?story_id=53179 (last visited March 7, 2014). These activities are fully consistent with the NRA's longstanding denunciation of violent extremism. *See NRA Disavows Connections With Groups Advocating Violence*, *American Rifleman*, Oct. 1964, at 72-73 (denouncing groups that support the overthrow or subversion of the government); Policy Statement of the National Rifle Association on Extremist Organizations and Militia Groups, May 23, 1995 (reaffirming the 1964 policy).

At the same time, the NRA has made clear its view that counter-terrorism efforts must be conducted within the bounds of the Constitution. *See, e.g., Terrorism Bill and Anti-Gun Exploiters*, *American Rifleman*, Aug. 1995, at 26 (denouncing "threats to privacy, freedom of association and other civil rights" in Clinton administration anti-terrorism proposals). Joining in a coalition with groups including the American Civil Liberties Union, the NRA supported an amendment to what later became the Anti-Terrorism and Effective Death Penalty Act of 1996, Pub. L. 104-132; one provision of the amendment struck language that would have allowed issuance of *ex parte* orders for business records of common carriers, public accommodations, storage facilities, or vehicle rental facilities. *See* H. Amdt. 950 to H.R. 2703, 104th Cong. (1996). Two years later, though, a new

version of the language that had been struck in 1996 was codified as 50 U.S.C. § 1862. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, § 602, 112 Stat. 2396, 2410-11 (1998). The government's interpretation and implementation of that provision—as amended by Section 215 of the USA PATRIOT Act, Pub. L. 107-56, § 215, 115 Stat. 272, 287-88 (2001), and now codified (with subsequent amendments) at 18 U.S.C. § 1861—is the subject of this case.

SUMMARY OF ARGUMENT

Since its decision in *Nat'l Ass'n for Advancement of Colored People v. State of Ala. ex rel. Patterson*, 357 U.S. 449 (1958), the Supreme Court has recognized that involuntary disclosure of the membership of advocacy groups inhibits the exercise of First Amendment rights by those groups. For nearly as long—since the debates leading up to enactment of the Gun Control Act of 1968—the Congress has recognized that excessive government recordkeeping on gun owners inhibits the exercise of Second Amendment rights. The mass surveillance program raises both issues. First, it could provide the government with the means of identifying members and others who communicate with the NRA and other Second Amendment advocacy groups. Second, it could provide the means of identifying gun owners without their knowledge or consent, contrary to longstanding

congressional policy—a policy that was repeatedly reaffirmed and strengthened by the very Congresses that enacted and reauthorized the legislation at issue in this case. The potential effect on gun owners’ privacy illustrates the potential effect of the government’s interpretation of the statute on other statutorily protected privacy rights. The decision below should therefore be reversed.

ARGUMENT

I. The Government’s mass surveillance program threatens the First Amendment rights of the NRA and its members.

For decades, the NRA’s legislative success has rested on its ability to inform its members and supporters, and to inspire those people to communicate, in turn, with policymakers at all levels of government. *See, e.g.,* C.B. Lister, *Firearms Laws in the 73d Congress*, *American Rifleman*, July 1934 at 17 (citing Roosevelt administration complaints about NRA communications on pending legislation); Edward H. Baker, *How the NRA Sets the Standard for Customer Engagement*, *strategy+business*, Dec. 19, 2013, *available at* <http://www.strategy-business.com/blog/How-the-NRA-and-Apple-Set-the-Standard-for-Customer-Engagement-A-QA-with-Peter-Murray?gko=ba413> (last viewed March 12, 2014) (describing NRA media and grassroots communications). That political effectiveness could be

drastically reduced by mass surveillance programs, which could have a “‘chilling’ effect,” *Gibson v. Florida Legislative Investigation Comm.*, 372 U.S. 539, 557 (1963), on communications between the NRA and its supporters. This concern is not unique to the NRA, but could apply equally with respect to the plaintiffs—or to any other organization that takes controversial stands on public issues.

A. The mass surveillance program could allow identification of NRA members, supporters, potential members, and other persons with whom the NRA communicates, potentially chilling their willingness to communicate with the NRA.

The Supreme Court made clear in *NAACP* that it had long “recognized the vital relationship between freedom to associate and privacy in one’s associations.” *NAACP*, 357 U.S. at 462. Because of that relationship, the “compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association” as the regulation of lobbying activities or the discriminatory taxation of certain newspapers. *Id.* Given “manifestations of public hostility” against a group, “compelled disclosure ... is likely to affect adversely the ability of [the group and its] members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate,” because the intrusion on privacy “may induce members to withdraw ... and dissuade others from

joining ... because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure.” *Id.* at 462-63. By making “group membership less attractive, [disclosure raises] First Amendment concerns about affecting the group’s ability to express its message.” *Rumsfeld v. Forum for Academic & Institutional Rights, Inc.*, 547 U.S. 47, 69 (2006).

Admittedly, some post-*NAACP* cases have been more deferential to government, focusing on the language in *NAACP* that noted members’ exposure “to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility” and requiring evidence of such harm to strike down disclosure regimes. *See, e.g., McIntyre v. Ohio*, 514 U.S. 334, 379 (1995); *Buckley v. Valeo*, 424 U.S. 1, 69 (1976). But the NRA and its members have certainly been subjected to “public hostility” from the highest levels of government, as well as from the media and other prominent elements of society. Individuals who are concerned about government monitoring of their communications might well avoid seeking information from a group that has been accused by the President of the United States of “spreading untruths,” and by the President’s press secretary of “repugnant and cowardly” advertising. *See Obama’s Remarks After Senate Gun Votes*, *The New York Times*, April 17, 2013; Michael D.

Shear, *White House Denounces Web Video by N.R.A.*, The New York Times, January 16, 2013. They might also be concerned about associating with a group of which the Vice-President of the National Education Association has said, “[t]hese guys are going to hell,” or which a journalism professor has accused of committing “treason ... worthy of the firing squad.” See Josh Richman, *Netroots Nation Features a Call to Action on Gun Control*, The Oakland Tribune, June 21, 2013; Christopher Swindell, *Gun safety debate is B.S.*, The Charleston Gazette, May 30, 2013.

Accordingly, like the NAACP, and for the same reasons, the NRA has jealously guarded information about its members and supporters. Those protective efforts have included litigation to challenge federal campaign finance laws that would have required disclosure of the names and addresses of certain contributors. See *McConnell v. Federal Election Comm’n*, 540 U.S. 93, 194-95 (2003). In *McConnell*, the executive vice-president of the NRA testified that “hundreds, if not thousands of individuals” had expressed concern to him about potential “repercussions either at work or in their community” if their NRA membership were disclosed. See Decl. of Wayne LaPierre, J.A., *McConnell v. Federal Election Comm’n*, 2003 WL 22070885, at *388. In the same case, the treasurer of the NRA’s political action committee testified that a “conspicuous and disproportionate” number

of contributors appear to limit their donations to avoid disclosure of their identities to the Federal Election Commission. For example, many contributors to the PAC “donate \$199.99, presumably because they are under the misimpression that the FEC’s disclosure requirement is triggered by annual donations at, rather than above \$200.” *See* Decl. of Mary Rose Adkins, Oct. 4, 2002, at 2, *Nat’l Rifle Ass’n v. Federal Election Comm’n* (Nos. 02-0581/02-0581) (D.D.C.).

The situation under the NSA’s mass surveillance program could be far worse. Under the campaign finance scheme at issue in *McConnell*, for example, potential NRA donors would at least have been on notice that their names and addresses would be disclosed, and could have chosen—albeit at the expense of reduced NRA effectiveness—to avoid disclosure by contributing at levels that would not trigger the disclosure requirement, or by not contributing at all. Here, the “disclosure” is both involuntary and universal, touching everyone who might communicate with the NRA or its affiliates by phone.

The involuntary “disclosure” would be even more chilling if, as widely reported, the NSA has engaged in other forms of mass surveillance not directly at issue in this case, but not foreclosed by the government’s interpretation—such as the gathering of e-mail headers, Internet browsing

information, and social media posts. *See* Letter from Ronald Weich to Sens. Dianne Feinstein and Saxby Chambliss, Feb. 2, 2011, *available at* http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf (last viewed March 10, 2014); Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'*, *The Guardian*, July 31, 2013. The same would be equally true for NSA tracking of mobile phone locations. *See* Barton Gellman and Ashkan Soltani, *NSA tracking cellphone locations worldwide, Snowden documents show*, *Washington Post*, Dec. 4, 2013.

Each of these programs standing on its own could provide the government with an extraordinary amount of information about those who communicate—for even the most innocent or praiseworthy reasons—with the NRA or any other group. Certainly, they would reveal a mosaic of individual activity far exceeding that which concerned Justice Sotomayor, who has “doubt[ed] that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year.” *United States v. Jones*, 132 S. Ct. 945, 957, 181 L. Ed. 2d 911 (2012) (Sotomayor, J., concurring). Just as the global position system monitoring struck down in *Jones* “generates a precise, comprehensive record of a person's public movements that reflects a

wealth of detail about her familial, political, professional, religious, and sexual associations,” *id.* at 955, so does the telephone metadata at issue in this case. Regardless of the form of data in question, “[a]wareness that the Government may be watching chills associational and expressive freedoms.” *Id.*

Under the programs revealed so far, the government may already possess information about everyone who has recently called the NRA by phone, e-mailed the NRA, or visited the NRA’s website, headquarters, satellite offices, or events. Conversely, the same programs would also gather information on potential members or donors contacted by phone or e-mail for NRA membership recruitment or fundraising programs, or for legislative or political reasons such as the transmission of legislative alerts or get-out-the-vote messages. The programs could also reveal at least the outlines of research and advocacy activities undertaken by NRA staff members, such as the websites visited in the course analyzing bills or preparing for litigation, or the identities of legislative staff members, outside attorneys, or potential litigants contacted by phone or e-mail.²

² Like the ACLU, the NRA sometimes supports “John Doe” lawsuits by persons wishing to vindicate their Second Amendment rights, but also fearing retribution. *See, e.g.,* NRA Institute for Legislative Action, *Case against Wilmington Housing Authority Moves to State Supreme Court*, available at <http://www.nraia.org/legal/articles/2014/case-against->

At the outer extreme, a location tracking program could reveal the identity of every mobile phone user who visits the NRA's headquarters—whether for a political or legislative event, or simply to use the NRA's shooting range or visit its National Firearms Museum. Similarly, location-tracking surveillance could reveal the travels of NRA staff members to engage in legislative or litigation meetings, political events, or other activities protected by the First Amendment. Any of these forms of tracking could easily reduce individuals' desire to interact with the NRA.

B. Modern data analysis techniques, and the risk of public disclosure, heighten First Amendment concerns about the mass surveillance program.

Government collection of identifying information about individuals is all the more threatening given advances in data aggregation and analysis techniques. *See generally* JA053-058 (Felten Decl. ¶¶ 47-64). The analysis of multiple data points and of combined types of data makes it possible to identify individuals from seemingly minor data. For example, according to one study, “Just four data points about the location and time of a mobile phone call ... make it possible to identify the caller 95 percent of the time.”

[wilmington-housing-authority-moves-to-state-supreme-court.aspx](#) (last viewed March 10, 2014) (describing public housing residents' challenge to housing authority firearms regulation).

James Risen and Eric Lichtblau, *How the U.S. Uses Technology to Mine More Data More Quickly*, The New York Times, June 8, 2013. These techniques have become commonplace in private industry, with one analysis firm holding as many as 1,500 data points on each of 500 million consumers worldwide. Natasha Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, The New York Times, June 16, 2012. Advanced data analysis techniques have also been widely heralded in the political world, with one consultant for President Obama's reelection campaign reporting that due to such techniques, "the campaign literally knew every single wavering voter in the country that it needed to persuade to vote for Obama, by name, address, race, sex and income." Jim Rutenberg, *Data You Can Believe In*, The New York Times, June 23, 2013.

Adding to the inherent danger of government access to such information, and of the unprecedented ability to use it to identify individuals, is the risk of public disclosure—which, in the Internet era, could make "a wealth of information" available to potential harassers. *See Doe v. Reed*, 130 S. Ct. 2811, 2825 (2010) (Alito, J., concurring). The government may argue that no such exposure is possible, or likely, due to the security measures surrounding the data. But those assurances are not comforting, given that the very existence of the phone records program was exposed by a lone ex-

contractor. See Glenn Greenwald, *et al.*, *Edward Snowden: the whistleblower behind the NSA surveillance revelations*, *The Guardian*, June 9, 2013. Further, under today's information-sharing policies, with enormous amounts of data routinely made available to low-level personnel, leaks of unprecedented scale may also become routine. See Marc Ambinder, *WikiLeaks: One Analyst, So Many Documents*, *National Journal*, Nov. 29, 2010 (describing access by Private First Class Bradley Manning to "intelligence streams from across the world"); Ellen Nakashima, *With better sharing of data comes danger*, *Washington Post*, Nov. 29, 2010 (describing leaks as the "downside to better information-sharing"). In fact, recent reports indicate that the mass surveillance program itself has been misused, both through the inevitable human errors that occur during the handling of enormous volumes of data by a large agency, and through outright abuse. See Barton Gellman, *NSA broke privacy rules thousands of times per year, audit finds*, *Washington Post*, Aug. 15, 2013 (describing unauthorized surveillance ranging "from significant violations of law to typographical errors that resulted in unintended interception of U.S. e-mails and telephone calls"); Siobhan Gorman, *NSA Officers Spy on Love Interests*, *Wall Street Journal*, Aug. 23, 2013. Thus, even if the information collection at issue in this case posed no threat in its own right, the risk of disclosure through

accident or abuse would make it unacceptable. The self-reporting and correction of error or abuse after the fact praised by the District Court, *see* SPA052, is cold comfort to those whose privacy has already been violated.

II. The Government's broad interpretation of Section 215 could circumvent legal protections for Americans' privacy, such as laws that guard against the registration of guns or gun owners.

The Congress and successive administrations have acted repeatedly to protect Americans' personal privacy in a variety of arenas. Many of these have now become routine parts of everyday life. We stand two paces back from one another at the pharmacy counter to avoid learning of our neighbors' medical issues, thanks to regulations under the Health Insurance Portability and Accountability Act. *See* 45 C.F.R. § 164.530(c) (2013). Both our surface mail and, ironically, our e-mail and the websites we visit bear a daily stream of federally mandated messages from credit card companies and others, notifying us of firms' privacy policies under the Financial Services Modernization Act, Pub. L. 106-102, 113 Stat. 1338 (1999), and other laws.

High among the privacy protections we enjoy—and illustrative of the mass surveillance program's potential to undercut legislative protection for privacy in other areas—are a number of provisions enacted in the past 35

years to protect gun owners' personal privacy, physical security, and freedom from any form of gun registration. Those provisions have been enacted out of well-founded concern for the potential misuse of such information, based on experience at home and abroad. In New York City, for example, rifle and shotgun registration lists have repeatedly been used to order the surrender or removal of firearms that had once been lawfully registered by their owners, but were later prohibited in the city due to design features or magazine capacity. See Edmund DeMarche, *NYPD cracks down on long guns that hold more than five rounds*, FoxNews.com, Dec. 5, 2013, available at <http://www.foxnews.com/us/2013/12/05/nypd-targets-owners-multi-clip-shotguns-rifles/> (last viewed March 12, 2014); David I. Caplan, *Firearms Registration And Waiting Periods: New York City's Lesson*, *American Rifleman*, Oct. 1993, at 67. See also David Kopel, *Who Needs Guns? Lessons From Down Under*, *Chronicles*, Oct. 2003 at 20 (describing confiscation and other restrictions following enactment of registration laws in Australia). Even if there were no threat of confiscation, the chance of public release of gun ownership information may threaten owners' safety. See, e.g., Timothy O'Connor and Meghan E. Murphy, *Journal News gun permit map used by burglars to target White Plains home?*, *Newsday*, Jan. 13, 2013 (describing burglary and attempted gun theft after a gun owner's

name and address were published online); Victor Fiorillo, *These Philadelphians Want Gun Permits*, Philadelphia, Aug. 15, 2012, available at <http://www.phillymag.com/news/2012/08/15/philadelphia-gun-permit-appeals-reasons/> (last viewed March 12, 2014) (noting that a city map of persons appealing firearms permit denials had been taken offline, and names redacted from previous versions of the article, due to “concerns over public safety”); *Lessons Learned in Database Incident*, Roanoke Times & World News, Mar. 25, 2007 (editorial expressing regret for publishing concealed handgun permit database containing addresses of “crime victims, law enforcement officers and domestic violence victims”).

Beyond implicating Second Amendment and public safety concerns, the Government’s interpretation of Section 215, as endorsed by the District Court, is a rule that defeats all exceptions, in violation of basic principles of statutory construction. Statutes should be read to avoid absurd results, *see S.E.C. v. Rosenthal*, 650 F.3d 156, 162 (2d Cir. 2011), and it would be absurd for Congress to adopt and maintain a web of statutes intended to protect against the creation of a national gun registry, while simultaneously authorizing the FBI or the NSA to gather records that could effectively create just such a registry, and potentially share them with other agencies as well. The real possibility of such abuse has already been documented

through other agencies' complaints about the lack of sharing by the NSA, and by apparent legal workarounds that have been used to cover otherwise unlawful sharing that does occur. *See* Eric Lichtblau and Michael S. Schmidt, *Other Agencies Clamor for Data N.S.A. Compiles*, New York Times, Aug. 3, 2013 (describing data requests from the Drug Enforcement Administration, Secret Service, Pentagon, Department of Homeland Security); Brian Fung, *The NSA is giving your phone records to the DEA. And the DEA is covering it up.*, The Washington Post, Aug. 5, 2013, available at <http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/05/the-nsa-is-giving-your-phone-records-to-the-dea-and-the-dea-is-covering-it-up/> (last viewed March 12, 2014).

The creation of a gun registry by use of telephone metadata or other records gathered through the NSA would effectively repeal the anti-registration provisions by implication—a prospect that is disfavored in general, and especially so “[w]here both laws are passed at the same session.” *Pullen v. Morgenthau*, 73 F.2d 281, 283 (2d Cir. 1934).³ As

³ The Government appears to have agreed with this view when it stated that Section 215 did not “clearly and explicitly” override privacy provisions of the Census Act. *See* Appellants’ Br. at 19. But the census statutes only expressly guard against unauthorized disclosure of census information by the government itself. *See* 13 U.S.C. §§ 9, 214. While pleased that the Government recognizes the policy against repeal by implication in this one context, the NRA is reluctant to assume that the

demonstrated below, the Congress has consistently acted to protect the privacy interests of gun owners, not only before the enactment of the Patriot Act and throughout the period in which the Act has been reauthorized and amended, but especially by acting—in the same year as the most recent reauthorization of the Patriot Act—to give permanent effect to several appropriations amendments directly touching on gun owners’ privacy. The District Court’s interpretation of Section 215 would allow all of these provisions to be effectively overridden at will, and is therefore implausible.

A. The Government’s interpretation of Section 215 would nullify statutory protections against centralization of gun ownership records.

At the outset of the modern debate over firearms regulation, the Gun Control Act of 1968 (GCA) created the first broad federal regulation of retail firearms sales in the United States. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, Title IV, 82 Stat. 197, 225 (1968); *amended by* Gun Control Act of 1968, Pub.L. 90-618, Title I, 82 Stat. 1213 (1968). During the 1968 debate, both the House and the Senate overwhelmingly voted down proposals to require registration of guns. 114 Cong. Rec. H22267 (daily ed. July 19, 1968); 114 Cong. Rec. S27420-421

Government would take a similar view of demands issued to non-governmental parties.

(daily ed. Sept. 18, 1968). Among the provisions eventually enacted, the GCA (under provisions still in effect, as amended) requires federally licensed firearms manufacturers, importers, and dealers to maintain records of all firearms made, imported, acquired or disposed of. Dealers are required to make those records available for inspection when necessary to enforce provisions of the GCA or to assist in tracing a firearm as part of a *bona fide* criminal investigation. *See generally* 18 U.S.C. § 923(g). As one senator put it, “The central compromise of the Gun Control Act of 1968—the *sine qua non* for the entry of the Federal Government into any form of firearms regulation was this: Records concerning gun ownership would be maintained by dealers, not by the Federal Government and not by State and local governments.” 131 Cong. Rec. S9163-64 (July 9, 1985) (statement of Sen. James McClure). The Firearms Owners’ Protection Act of 1986, Pub. L. No. 99-308, 100 Stat. 449 (1986) amended the GCA to further protect gun owners’ privacy, by specifying that no subsequently enacted “rule or regulation “may require centralization of federally mandated dealer records, or require establishment of “any system of registration of firearms, firearms owners, or firearms transactions or dispositions.” 18 U.S.C. § 926(a).

In addition to concerns about dealer records, the Congress has been concerned about the potential misuse of background check information

gathered during firearms transfers. The Brady Handgun Violence Prevention Act of 1993, Pub. L. No. 103–159, 107 Stat. 1536 (1993), further amended the GCA by creating the National Instant Criminal Background Check System (NICS), and specifies that the NICS “shall . . . destroy all records of the system with respect to the call (other than the [transaction] identifying number and the date the number was assigned) and all records of the system relating to the person or the transfer.” 18 U.S.C. § 922(t)(2)(C). Section 103(i) of the Act also prohibits use of the NICS to create a federal gun registration system:

Prohibition Relating To Establishment of Registration Systems With Respect To Firearms. No department, agency, officer, or employee of the United States may—

(1) require that any record or portion thereof generated by the system established under this section may be recorded at or transferred to a facility owned, managed, or controlled by the United States or any State or political subdivision thereof; or

(2) use the system established under this section to establish any system for the registration of firearms, firearm owners, or firearm transactions or dispositions except with respect to person, prohibited by section 922 (g) or (n) of title 18, United States Code State law, from receiving a firearm.

107 Stat. at 1542.

Even courts upholding broad interpretations of Congress’ powers under the GCA have recognized that the Government’s power to gather dealers’ records must end somewhere. *See, e.g., Nat’l Shooting Sports*

Found., Inc. v. Jones, 716 F.3d 200, 212-13 (D.C. Cir. 2013) (upholding demand for dealers’ records as too limited to be restricted by 18 U.S.C. § 926(a) and appropriations amendments on centralizing purchase records).

The broad view of Section 215 adopted by the District Court, however, would implicitly override these longstanding protections. Requests for “firearms sales records” are expressly provided for in the statute, albeit at a higher level of sign-off within the FBI, *see* 50 U.S.C. § 1861(a)(2)—but as the District Court put it, the Government’s burden to successfully press a Section 215 request “is not substantial.” SPA033. If the Government can request all available data simply because it does not “know which particle ... will lead to useful counterterrorism information,” SPA035, the Government could simply assert that it is necessary to seek all firearms dealers’ sales records, all NICS transaction information, or any subset of either, in order to facilitate later searching in connection with an anti-terrorism or counter-intelligence investigation. It strains credulity to think that the Congress could have intended that result while other provisions remain on the books that “clearly demonstrate[] Congress’ concern about any attempt by [the Bureau of Alcohol, Tobacco and Firearms] to establish a national firearms registry.”

RSM, Inc. v. Buckles, 254 F.3d 61, 67 (4th Cir. 2001) (discussing 18 U.S.C. § 926(a)).⁴

B. The Government’s interpretation of Section 215 conflicts with contemporaneously enacted protections for gun owners’ privacy.

In amendments to various appropriations acts, the Congress has also used its spending power to protect gun owners’ privacy against government accumulation of firearms ownership records. Tellingly, several of these provisions have been reenacted—and strengthened—since the enactment of Section 215.

First, in response to a regulation proposed by the Carter administration that would have required centralized federal reporting of all gun sales by federal firearms licensees, Firearms Regulations, 43 Fed. Reg. 11,800 (Mar. 21, 1978), every appropriations bill since fiscal year 1979 funding the Bureau of Alcohol, Tobacco, and Firearms (now the Bureau of

⁴ It might be argued that FBI or NSA use of such information would be for different purposes than ATF use, but the policy concerns that have inspired anti-registration provisions are not specific to any one agency—a fact demonstrated by the limits Congress placed on FBI use of background check records. *See supra* pp. 20-21. And the ATF is, after all, not a second fiddle to the FBI, but the primary agency “responsible for investigating ... criminal and regulatory violations of the Federal firearms ... laws.” Homeland Security Act of 2002, Pub. L. 107–296, 116 Stat 2135, § 1111(b) (2002).

Alcohol, Tobacco, Firearms, and Explosives) has contained a funding restriction to prevent such activities. An Act making appropriations for the Treasury Department, the United States Postal Service, the Executive Office of the President, and certain Independent Agencies, for the fiscal year ending Sept. 30, 1979, and for other purposes. Pub. L. No. 95–429, 92 Stat 1001 (1978).

In the same year as the most recent reauthorization of the Patriot Act, *see* PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, § 2(a), 125 Stat. 216 (2011), the 112th Congress made that provision permanent.

The FY 2012 provision reads:

[N]o funds appropriated herein *or hereafter* shall be available for salaries or administrative expenses in connection with consolidating or centralizing, within the Department of Justice, the records, or any portion thereof, of acquisition and disposition of firearms maintained by Federal firearms licensees[.]

Consolidated and Further Continuing Appropriations Act, 2012, Pub. L. No. 112-55, 125 Stat. 552, 609 (2011) (emphasis added).

Similarly, while federal law requires licensed firearms dealers, manufacturers and importers to surrender their business records to the ATF when they go out of business, *see* 18 U.S.C. § 923(g)(4), the Congress has enacted a provision every year since FY 1997 to ensure that these records

are not indexed by the name of the buyer. The 112th Congress made this protection permanent, too, beginning in FY 2012:

[H]ereafter, no funds made available by this *or any other* Act may be used to electronically retrieve information gathered pursuant to 18 U.S.C. 923(g)(4) by name or any personal identification code[.]

125 Stat. 552, 610 (emphasis added).

Records that are created in the course of tracing firearms may also contain information on individual gun buyers. To protect the privacy of this information, the Congress enacted a series of appropriations amendments beginning in FY 2003. *See* Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, § 644, 117 Stat. 11,473-74 (2003). And once again, the 112th Congress made this protection permanent beginning in FY 2012:

[D]uring the current fiscal year *and in each fiscal year thereafter*, no funds appropriated under this or any other Act may be used to disclose part or all of the contents of the Firearms Trace System database maintained by the National Trace Center of the Bureau of Alcohol, Tobacco, Firearms and Explosives or any information required to be kept by licensees pursuant to section 923(g) of title 18, United States Code, or required to be reported pursuant to paragraphs (3) and (7) of such section[.]

125 Stat. 552 at 609 (emphasis added).

Finally, in response to a regulatory proposal that would have allowed retention of background transaction records for 90 days, *see* National Instant Criminal Background Check System Regulation, 64 Fed. Reg. 10260-02 (March 3, 1999), the Congress passed an additional limit on such retention,

which has been included in every Justice Department bill since FY 1999. *See Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Pub. L. No. 105–277, § 621, 112 Stat 2681, 2797 (1998).* And again, the 112th Congress made that provision permanent:

Hereafter, none of the funds appropriated pursuant to this Act or any other provision of law may be used for

(2) any system to implement subsection 922(t) of title 18, United States Code, that does not require and result in the destruction of any identifying information submitted by or on behalf of any person who has been determined not to be prohibited from possessing or receiving a firearm no more than 24 hours after the system advises a Federal firearms licensee that possession or receipt of a firearm by the prospective transferee would not violate subsection (g) or (n) of section 922 of title 18, United States Code, or State law[.]

125 Stat. 552 at 632 (emphasis added).

As with the statutory provisions previously discussed, the Congresses that reenacted and strengthened all of these protections could not have acquiesced in an interpretation of Section 215 that would make those same protections meaningless. Under the government’s reading of Section 215, the government could simply demand the periodic submission of all firearms dealers’ transaction records, then centralize them in a database indexed by the buyers’ names for later searching. The successive Congresses that

enacted and strengthened these provisions could not have intended to allow that.

C. The Government's interpretation of Section 215, coupled with the potential gathering and aggregation of other forms of data, could allow the easy identification of gun owners, contrary to all privacy protections enacted by Congress.

Due to all of these preexisting protections, the NRA generally remained neutral during debates on the Patriot Act, supporting only a few limited provisions to enhance protection for gun owners under Section 215. But that position was a result of a far more limited view of the plain language of the Act than the Government now adopts. If the Government's authority to collect phone company metadata is as broad as the District Court has found, nothing would prevent it from obtaining other forms of metadata, such as information on website traffic, or credit card records, and it has reportedly done just that. *See* Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'*, *supra* p. 7; Martha C. White, *Big Brother Is Watching You Swipe: The NSA's Credit Card Data Grab*, *Time*, June 11, 2013.

Gathering and aggregating such private-sector records could allow the government to create a far more complete registry of actual or likely gun owners than could be created with government-mandated information—

rendering all debate over the scope of legislative privacy protections meaningless. For example, a person whose phone records show a pattern of repeated calls to gun stores, shooting ranges, and the NRA, is considerably more likely to be a gun owner than a person who makes no such calls. If phone records are combined with other information, far more detailed profiles could be assembled; if a person not only calls gun stores, ranges, and the NRA, but also visits hunting-related websites, makes credit card purchases from shooting sports retailers, and travels to firing ranges, it could be predicted with near certainty that he or she is a gun owner. The value of such information in identifying likely gun owners might dwarf the importance of an ATF record of a firearm purchased years ago from a now-defunct dealer, or a NICS transaction record showing transfer of a firearm that may have been sold or given away as a gift. If the Congress felt the latter records were worthy of protection, it surely could not have envisioned the Government's assumption of far broader powers under Section 215.

CONCLUSION

The District Court's broad reading of Section 215 raises serious concerns about the section's effect on the First Amendment rights of gun owners and their organized representatives, through the potential for

monitoring and possibly exposing their communications. If programs like those currently approved by the District Court's decision are allowed to continue and grow unchecked, they could also—contrary to clear congressional intent—undo decades of legal protection for the privacy of Americans in general, and of gun owners in particular. Accordingly, this Court should reverse the judgment of the District Court, and remand the matter for entry of a preliminary injunction.

Dated: March 13, 2014

Respectfully submitted,

/s/ John Frazer

John Frazer
Law Office of John Frazer, PLLC
3925 Chain Bridge Road, Suite 403
Fairfax, VA 22030
Phone: (703) 352-7276
Fax: (703) 359-0938
jfrazer@jfrazerlaw.com

**CERTIFICATE OF COMPLIANCE WITH TYPE-
VOLUME LIMITATION, TYPEFACE REQUIREMENTS, AND
TYPE STYLE REQUIREMENTS**

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 6,135 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

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 it has been prepared in a proportionally spaced typeface using Microsoft Word for Windows 2010 in 14-point Times New Roman type.

/s/ John Frazer
Attorney for National Rifle
Association of America, Inc.

Dated: March 13, 2014