

Laura Rótolo
Staff Attorney
ACLU of Massachusetts
211 Congress Street
Boston, MA 02110
(617) 482-3170 x311
lrrotolo@aclum.org

March 25, 2010

Transportation Security Administration
Freedom of Information Act Office, TSA-20
11th Floor, East Tower
601 South 12th Street
Arlington, VA 20598-6020

To whom it may concern:

This letter constitutes a request pursuant to the Freedom of Information Act, 5 U.S.C. § 552 made to the Transportation and Security Administration. The Request is submitted on behalf of the American Civil Liberties Union of Massachusetts and its educational arm, the American Civil Liberties Union Foundation of Massachusetts (jointly referred to as ACLUM).

I. BACKGROUND

The Transportation Security Administration has statutory responsibility and authority for ensuring the security of all modes of transportation, including, among others, civil aviation, ferries, passenger rail, and mass transit. 49 U.S.C. § 114(d), and has been directed to make use of new technologies in all of those environments. 49 U.S.C. § 114(f).

In dealing with air travel safety alone, TSA employs over 48,000 Transportation Security Officers at hundreds of airports across the country to screen passengers and their baggage using an array of technologically advanced systems such as advanced technology x-ray systems, walk-through metal detectors, explosive trace detection equipment, trained canines, vapor trace machines that detect liquid explosives, Advanced Imaging Technology and explosives detection systems. The high-tech screening works in tandem with individual officers engaged in bomb appraisal, detection of suspicious behavior, and the search of individual passengers, including full-body pat-downs. These

measures are not limited to the screening of passengers entering boarding areas but extend as well to all public areas of airports.¹

Given its connection to the events of 9/11, security at Logan International Airport in Boston has figured prominently in TSA air travel safety measures. Among other steps, TSA has installed three AIT whole body scanning portals in Logan's Terminal A with more apparently ordered. It has also been reported that Logan is one of only a few airports where TSA has deployed the SPO-7, a so-called stand-off device that employs millimeter wave technology to screen individuals outside sterile areas. TSA has assigned a number of Behavior Detection Officers (BDOs) to Logan. Automobiles entering the parking garage in Logan's Terminal B are subject to search upon entry.

The implementation of these measures, particularly as they move beyond the screening of passengers, raise significant public questions about their increasing intrusion on personal privacy and their effectiveness in increasing public safety, to say nothing of their high cost and their safety. Yet these measures often have been rolled out with little or no public input until they are already in use. Indeed some of these new technologies have been procured and implemented at lightning speed in response to past breaches of security. For example, in response to the December 25, 2009, attempted attack on Northwest flight 253, TSA increased its planned deployment of Whole Body Imagers from 878 to 1,800 units and began using them as a primary screening measure.²

Among these technologies are Advanced Imaging Technology (AIT) – also known as the Whole Body Imager or Backscatter technology; Millimeter Wave /Standoff technology; Explosives Trace Portal (ETPs) and potentially thermal imaging devices. Whole Body Imagers, for example, have caused privacy concerns over the images of the naked body that are produced, specifically who has access to the images, if they are stored and if the passengers can be identified. In addition, there are concerns about its effectiveness. On March 17, 2010, GAO official Steve Lord testified to the House Homeland Security Committee that it was unclear whether the scanners would have detected the December incident. According to the GAO, TSA has conducted a life-cycle cost estimate and an alternatives analysis for the AIT, but not a cost-benefit analysis of the original deployment strategy or the revised AIT deployment strategy. The GAO testified that TSA should conduct such a study, citing an estimate that staffing costs alone could add up to \$2.4 billion over the expected service life of the machines.³

¹ Testimony of Secretary Napolitano before the Senate Committee on the Homeland Security and Governmental Affairs, "Intelligence Reform: The Lessons and Implications of the Christmas Day Attack" (Written Testimony), January 20, 2010, available at http://www.dhs.gov/ynews/testimony/testimony_1264015592011.shtm

² Government Accountability Office, Testimony Before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, House of Representatives, March 17, 2010, GAO-10-484T.

³ *Id.*

As TSA moves beyond the “sterile area” of the airport and even beyond the airport perimeter, the public will continue to have questions and concerns about the safety of new technologies, the privacy safeguards and the cost-benefit analysis of employing many of these methods.

In order to provide more information to the public about how these technologies and methods work in practice, this request seeks documents containing data underlying various of these measures.

II. DOCUMENTS SOUGHT

Whole Body Imaging/ Backscatter/ Advanced Imaging Technology (AIT)

1. Any life-cycle cost estimate and alternatives analysis pertaining to AIT, any cost-benefit study, risk management study or other study of effectiveness of the full body scanners.
2. Documents showing the procedure used to select passengers who are to be subjected to AIT screening and procedures for determining whether AIT is used as a primary versus secondary screening method. Training documents for TSA personnel regarding the selection of passengers to be subjected to AIT screening.
3. Any standard operating procedures, rules, guidelines and training documents for TSA personnel regarding the operation of AIT, specifically as they relate to privacy of passengers subjected to this screening.
4. Any rules, guidelines, protocols, standard operating procedures and/or recommendations regarding the retention and/or deletion of images produced by AIT; any agreements between TSA or the Department of Homeland Security and AIT manufacturers regarding the retention and/or deletion of images produced by AIT.
5. Any rules, guidelines, protocols, standard operating procedures, recommendations and/or agreements with manufacturers regarding radiation levels, specifically whether factory settings of radiation levels can be changed by TSA personnel.
6. Any rules, guidelines, protocols, standard operating procedures and/or recommendations regarding the machines’ connectivity to the internet and relation of the machines to internal or external databases.
7. Documents showing how many AIT units are deployed at Logan International Airport, including which terminals currently have and/or are scheduled to receive

AIT units.

Passive Millimeter Wave Technology / Standoff technology

8. Any reports of studies or assessments regarding the use of Passive Millimeter Wave Technology / Standoff technology (herein “Standoff Technology”) in airports in Denver and Minneapolis.
9. Contracts between TSA or Logan Airport authorities and QinetiQ for the provision of Standoff Technology.
10. Documents regarding the use of Standoff Technology at Logan International Airport, including lists of numbers of units used and terminals currently using the technology.
11. Any life-cycle cost estimates, alternatives analysis reports, cost-benefit studies and/or risk management studies relating to the use of Standoff Technology.
12. Documents showing the text of any signage used alerting persons that Standoff Technology is being implemented.
13. Any standard operating procedures, rules, guidelines and training documents for TSA personnel regarding the privacy of persons subjected to Standoff Technology.

Explosives Trace Portal (ETP)

14. Any reports addressing the effectiveness or performance of ETPs. Documents addressing performance issues that have led to ETPs being removed from some airports.

Thermal Imaging Technology

15. Any documents describing the potential for use of thermal imaging technology to detect illness at Logan Airport.

Behavior Detection Officers (BDOs) at Logan Airport

16. Any standard operating procedures, rules, guidelines and training documents for BDO officers at Logan Airport; any training materials regarding the use of

voluntary and non-voluntary stops of persons outside the “sterile” area beyond passenger screening points.

III. SEARCH AND COPYING FEES

The American Civil Liberties Union Foundation of Massachusetts (“ACLUM”) requests a waiver of search, duplication and review fees under the FOIA statute and Department of Homeland Security Regulations for two reasons. First, the requester qualifies as a representative of the news media. Second, release of the records requested is in the public interest and not in any commercial interest of the requester.

1. ACLUM is entitled to a waiver of fees because it is a representative of the news media as defined in the FOIA statute and in DHS regulations.

The requester is a representative of the news media under both the FOIA statute and the Department of Homeland Security regulations regarding FOIA fees in that it is an organization “actively gathering news for an entity that is organized and operated to publish or broadcast news to the public,” where “news” is defined as “information that is about current events or that would be of current interest to the public.” 5 U.S.C. § 552(a)(4)(A)(ii)(II); 6 C.F.R. § 5.5(b)(6).

In addition, ACLUM meets the statutory definition of a “representative of the news media” because it is an “an entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn raw materials into a distinct work, and distributes that work to an audience.” *Nat’s Security Archive v. Dep’t of Defense*, 880 F.2d 1381, 1387 (D.C. Cir 1989). *See also Electronic Privacy Information Ctr. v. Dep’t of Defense*, 241 F.Supp. 2d 5, 10-15 (D.D.C. 2003) (finding non-profit interest group that disseminated an electronic newsletter and published books was a “representative of the media” for purposes of FOIA.)

ACLUM, a not-for-profit, non-partisan organization with over 22,000 members and supporters across Massachusetts is dedicated to the principles of liberty and equality. As the Massachusetts affiliate of the national ACLU, a not-for-profit, non-partisan organization with over 500,000 members nationwide, ACLUM distributes information outside of Massachusetts to thousands of members of the public.

Gathering and disseminating current information to the public is a critical and substantial component of ACLUM’s mission and work. ACLUM publishes newsletters, news briefings, reports and other printed materials that are disseminated to the public. *See* Exhibits A – C. These materials are widely available to everyone, including tax-exempt organizations, not-for-profit groups, law students and faculty, at no cost. ACLUM also disseminates information through its heavily subscribed website, www.aclum.org, a blog, <http://www.massrightsblog.org> and regular posts on social media sites such as Facebook and Twitter. *See* Exhibits D – F. Our web postings address civil liberties issues in depth,

provide features on civil liberties issues in the news, and contain hundreds of documents that relate to the issues addressed by ACLUM. The website includes features on information obtained through the FOIA. *See, e.g.,* www.aclum.org/ice.

Courts have further confirmed the broad scope of the definition of news media. In a case regarding a request made by a similar advocacy organization, the Electronic Privacy Information Center, the D.C. Circuit held that “[i]t is critical that the phrase ‘representative of the news media’ be broadly interpreted if the act is to work as expected . . . I[n] fact, any person or organization which regularly publishes or disseminates information to the public . . . should qualify for waivers as a ‘representative of the news media.’” *Electronic Privacy Information Ctr. v. Dep’t of Defense*, 241 F.Supp. 2d 5, 10 (D.D.C. 2003).

Other organizations similar to ACLUM have also been found to meet the statutory definition of “representative of the news media” when the organization making the request is “an entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn raw materials into a distinct work, and distributes that work to an audience.” *Nat’l Security Archive v. Dep’t of Defense*, 880 F.2d 1381, 1387 (D.C.Cir 1989) (finding that organization was a “representative of the news media”); *See also Electronic Privacy Information Ctr. v. Dep’t of Defense*, 241 F.Supp. 2d 5, 10-15 (D.D.C. 2003) (holding that non-profit public interest group that disseminated an electronic newsletter and published books was a “representative of the media” for purposes of FOIA).

Gathering, analyzing and disseminating information that is relevant and current to issues relating to civil liberties and privacy are key components of ACLUM. The organization continually and as part of its core functions disseminates information of public interest through internet, print, television and radio. Such information reaches thousands of members of the public including students, journalists, academics, advocates, members of government and interested readers every year.

These characteristics are typically sufficient to convey “representative of the news media” status on FOIA requesters. Courts have held that “[i]t is critical that the phrase ‘representative of the new media’ be broadly interpreted if the act is to work as expected . . . I[n] fact, any person or organization which regularly publishes or disseminates information to the public . . . should qualify for waivers as a ‘representative of the news media.’” *Electronic Privacy Ctr. v. Dep’t of Defense*, 241 F.Supp, 2d 5, 10 (D.D.C. 2003).

On account of these factors, government agencies have waived fees for the ACLU and ACLUM on numerous occasions.⁴

2. The records sought are in the public interest and the requester has no commercial interest in the disclosure.

ACLUM is entitled to a waiver or reduction of fees because “[d]isclosure of the requested information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government,” and “[d]isclosure of the information is not primarily in the commercial interest of the requester.” 5 U.S.C. § 552(a)(4)(A)(iii); 6 CFR § 5.5(k)(1)(i) and (ii).

This request aims at furthering public understanding of government conduct, and specifically at helping the public determine the ways in which especially the Transportation Security Administration, is carrying out security functions at airports and other travel-related locations. It therefore meets the component spelled out in 6 CFR § 5.5(k)(2)(iii).

There is broad demonstrated public interest in the safety, privacy impact, cost and effectiveness of new technologies and tools that TSA is implementing. 6 CFR § 5.5(k)(1)(iii). Countless news articles, opinion pieces, blogs and internet posts have been dedicated to this subject. A selection of such articles is included in Exhibit G. *See e.g.* Anita Allen, *Privacy Stays Home This Year: The Moralist*, The Star-Ledger, December 10, 2006; James Bamford, *Who's in Big Brother's Database?*, The New York Times, November 5, 2009; Jeffrey Rosen, *Nude Awakening*, The New Republic, February 10, 2010; Marc Rotenberg, *Opposing View: Uniquely Intrusive Devices*, USA Today, January 12, 2010; Bruce Schneier, *Our Reaction Is the Real Security Failure*, AOL News, January 7, 2010; Bruce Schneier, *Stop the Panic on Air Security*, CNN, January 7, 2010; Spencer S. Hsu, *Scanners may not have detected alleged explosive in Detroit jet case*, GAO reports, Washington Post, March 18, 2010; Jaikumar Vijayan, *Travelers file complaints over TSA body scanners*, Business Week, March 8, 2010; Will Pavia, *Muslim woman refuses body scan at airport*, London Times Online, March 3, 2010; Jaikumar Vijayan, *Suspend airport body scanner program, privacy groups say*, Computerworld, February 26, 2010; Julie Johnsson, *Airport body scanners have critics, including Pope*, Chicago

⁴ The following are examples of requests in which government agencies did not charge the ACLU or ACLUM fees associated with responding to a FOIA request: (1) Immigration and Customs Enforcement granted the ACLU of Massachusetts a waiver of all search fees for a request submitted on Jan. 25, 2007; (2) The Office of Science and Technology Policy in the Executive Office of the President told the ACLU that it would waive the fees associated with a FOIA request submitted by the ACLU in August 2003; (3) The Federal Bureau of Investigation did not charge the ACLU fees associated with a FOIA request submitted by the ACLU in August 2002; (4) The Office of Intelligence Policy and Review did not charge the ACLU fees associated with a FOIA request submitted by the ACLU in August 2002; and (5) The Office of Information and Privacy in the Department of Homeland Security did not charge the ACLU fees associated with a FOIA request submitted by the ACLU in August 2002.

Tribune, February 23, 2010; Thomas Frank, *Airport-security plan calls for 500 body scanners in '11*, USA TODAY, February 3, 2010; *European Union Puts Off Reply to U.S. Body Scanner Request*, AFP, January 21, 2010; *Body Scanners Risk Right to Privacy Says UK Watchdog*, BBC, January 20, 2010; *The Body Scanner Scam*, The Wall Street Journal, January 18, 2010; *The Fight Against Full-Body Scanners in Airports*, Los Angeles Times, January 13, 2010; *Mixed Signals on Airport Scanners*, The New York Times, January 12, 2010; *Body Scanners Can Store, Send Images, Group Says*, CNN, January 11, 2010; *European Response Mixed to New U.S. Security Demands*, Business Week, January 4, 2010; *Schiphol Buys 60 Body Scanners, Denies Lax Security*, Reuters, January 4, 2010; *New Scanners Break Child Porn Laws*, The Guardian, January 4, 2010; *TSA Tries to Assuage Passengers' Concerns About Full Body Scans*, The Washington Post, January 4, 2010; *Brown Gives Go-Ahead for Full Body Scanners at Britain's Airports*, The Guardian, January 4, 2010; *Former Homeland Security Chief Argues for Whole-Body Imaging*, The Washington Post, January 1, 2010; *150 More Full-Body Scanners to go in U.S. Airports*, CNN, December 31, 2009; *Calls for Full-Body Scanners Re-Ignite Privacy Concerns*, Fox News, December 31, 2009; *Body Scanners Not 'Magic Technology' Against Terror*, CNN, December 31, 2009; *Wide Use of U.S. Airport Body Scanners Depends on Obama*, Reuters, December 30, 2009; *Do Airport Imagers Invade Privacy*, The San Francisco Chronicle, December 29, 2009; *No more getting naked for the TSA*, The Examiner, May 20, 2009; *X-Ray Body Scanner Stirs Controversy*, Fox Washington DC, May 18, 2009; *Airport scanners take 'naked' pics, group says*, CNN.com, Monday, May 18, 2009; Kai Jackson, *Total Body Scans At Airports Cause Controversy*, Channel 13 Baltimore, May 18, 2009; *Whole Body Imaging is Wholly Frightening*, Manolith.com, Monday, May 18, 2009; *Commentary: Whole-Body imaging invades privacy*, CNN.com, May 19, 2009; *Privacy Advocates Take Issue With 'Whole Body Imaging' Airport Security Technology*, All Headline News, May 19, 2009; *Airport scanners take 'naked' pics, group says*, CNN.com, Monday, May 18, 2009; *Airport body scans: An issue of privacy*, The Windsor Star (Canadian), Tuesday, May 12, 2009; Anice Tibbetts, *Airport officials make plans to conduct virtual strip searches*, CanWest News Service, May 6, 2009; David Copeland, *Scanner finds hidden objects, not flesh*, Boston.com, April 27, 2009; *Herald Poll: Porn at the airport?* Daily Herald, April 24, 2009; *Chaffetz wants ban on airport whole body imaging*, ABC Channel 4 (Salt Lake City), April 22, 2009; William Saletan, *Deeper Digital Penetration*, Slate, April 8, 2009; Sean O'Neill, *TSA: Whole-body scanners to replace metal detectors*, Budget Travel, April 7, 2009; Joe Sharkey, *Whole-Body Scans Pass First Airport Tests*, N.Y. Times, April 6, 2009; Jeremy Hsu, *Airport body scans reveal all*, MSNBC, Apr. 1, 2009; *New security scan at DFW Airport has privacy advocates worried*, Dallas Morning News, June 16, 2008; Thomas Frank, *TSA looks into using more airport body scans*, USA Today, October 7, 2007; William Saletan, *Digital Penetration*, Slate, Mar. 3, 2007; *Controversial X-ray machine to make national debut Friday at Sky Harbor*, Associate Press, February 21, 2007; *Phoenix Airport to Test X-Ray Screening*, Associate Press as reported on Privacy.org, December 1, 2006; Joe Sharkey, *Airport screeners could see X-rated X-Rays*, New York Times, May 24, 2005; Thomas Frank, *Airports roll out high-tech security*, USA Today, May 16, 2005; Ryan

Single, *New Screening Technology Is Nigh*, Wired News, May 19, 2005; Bryon Okada, *TSA official says machine, not screeners, at fault*, Star-Telegram, May 1, 2005; Michael Grabell, *Airport plans to screen for explosives this fall Machines at D/FW*, Dallas News, May 1, 2005; Ryan Single, *Passenger Screening, Take 10*, Wired News, January 31, 2005; *'Nice Bombs Ya Got There'*, Associated Press, Wired News, June 26, 2003; Megan Lisagor, *TSA awards passenger screening contract*, Federal Computer Week, March 10, 2003; Megan Lisagor, *TSA prepares passenger screening system*, Federal Computer Week, February 26, 2003; *Smart Check-In Cuts Airport Lines*, Wired News, February 5, 2001.

As the federal government announces the spending of multiple millions of dollars on new technologies and subjects passengers to ever-increasing security screenings, the public has demanded answers to a host of questions. How safe are these technologies? Are they necessary? Do they violate the privacy of travelers? Do they work? Are they the best way to spend our tax money in these tight economic times? Many of these answers can only be answered through an analysis of the documents requested here. For these reasons, the disclosure is very “‘likely to contribute’ to an understanding of government operations or activities” and this contribution is likely to be “significant” given the lack of publicly available information on the subject. 6 C.F.R. § 5.5(k)(2)(ii) and (iv).

Lastly, ACLUM is a non-profit organization whose purposes are the protection of civil rights and liberties and to advance a just, democratic, and pluralistic society. As such, the requesters have no “commercial interest” in the information. 6 CFR § 5.5(k)(1)(ii).

IV. APPLICATION FOR EXPEDITED PROCESSING

ACLUM respectfully seeks expedited processing of its request for public records for the reasons laid out below and in a certified statement attached as Exhibit H.

We request expedited processing pursuant to 5 U.S.C. § 552(a)(6)(E) and 6 C.F.R. § 5.5(d). There is an urgency to inform the public about the government activities addressed in the request and the requester is an organization primarily engaged in disseminating such information. *See* 6 C.F.R. § 5.5(d)(1)(ii).

1. There is an urgency to inform the public about a federal government activity.

The records sought relate to “an alleged government activity” – the tools and methods TSA uses to address airport safety. 6 C.F.R. § 5.5(d)(1)(ii). Passenger screening

and airport security are tasks carried out almost exclusively by the federal government. They are funded by Congress and have a daily impact on the general public.

There is an urgent need to inform the public about these government activities because in the last few years, the federal government has vastly expanded the way it addresses airport security, with new technologies and an expansion of screening beyond the “sterile” area beyond security screening points. These activities implicate core privacy concerns, but many unanswered questions remain. The public has raised questions regarding the standards that guide or limit these new technologies, including whether they are potentially invasive, unsafe or subject to abuse. Without disclosure of the records sought, the public will remain in the dark about TSA’s operations, and cannot assess for itself whether the programs are necessary, effective, or subject to sufficient limits and oversight.

The urgent need for information is demonstrated by the countless news articles, opinion pieces, blogs and internet posts that have been dedicated to this subject in the recent months. A selection of such articles is included in Exhibit G. *See e.g.* Anita Allen, *Privacy Stays Home This Year: The Moralist*, The Star-Ledger, December 10, 2006; James Bamford, *Who's in Big Brother's Database?*, The New York Times, November 5, 2009; Jeffrey Rosen, *Nude Awakening*, The New Republic, February 10, 2010; Marc Rotenberg, *Opposing View: Uniquely Intrusive Devices*, USA Today, January 12, 2010; Bruce Schneier, *Our Reaction Is the Real Security Failure*, AOL News, January 7, 2010; Bruce Schneier, *Stop the Panic on Air Security*, CNN, January 7, 2010; Spencer S. Hsu, *Scanners may not have detected alleged explosive in Detroit jet case, GAO reports*, Washington Post, March 18, 2010; Jaikumar Vijayan, *Travelers file complaints over TSA body scanners*, Business Week, March 8, 2010; Will Pavia, *Muslim woman refuses body scan at airport*, London Times Online, March 3, 2010; Jaikumar Vijayan, *Suspend airport body scanner program, privacy groups say*, Computerworld, February 26, 2010; Julie Johnsson, *Airport body scanners have critics, including Pope*, Chicago Tribune, February 23, 2010; Thomas Frank, *Airport-security plan calls for 500 body scanners in '11*, USA TODAY, February 3, 2010; *European Union Puts Off Reply to U.S. Body Scanner Request*, AFP, January 21, 2010; *Body Scanners Risk Right to Privacy Says UK Watchdog*, BBC, January 20, 2010; *The Body Scanner Scam*, The Wall Street Journal, January 18, 2010; *The Fight Against Full-Body Scanners in Airports*, Los Angeles Times, January 13, 2010; *Mixed Signals on Airport Scanners*, The New York Times, January 12, 2010; *Body Scanners Can Store, Send Images, Group Says*, CNN, January 11, 2010; *European Response Mixed to New U.S. Security Demands*, Business Week, January 4, 2010; *Schiphol Buys 60 Body Scanners, Denies Lax Security*, Reuters, January 4, 2010; *New Scanners Break Child Porn Laws*, The Guardian, January 4, 2010; *TSA Tries to Assuage Passengers' Concerns About Full Body Scans*, The Washington Post, January 4, 2010; *Brown Gives Go-Ahead for Full Body Scanners at Britain's Airports*, The Guardian, January 4, 2010; *Former Homeland Security Chief Argues for Whole-Body Imaging*, The Washington Post, January 1, 2010; *150 More Full-Body Scanners to go in*

U.S. Airports, CNN, December 31, 2009; *Calls for Full-Body Scanners Re-Ignite Privacy Concerns*, Fox News, December 31, 2009; *Body Scanners Not 'Magic Technology' Against Terror*, CNN, December 31, 2009; *Wide Use of U.S. Airport Body Scanners Depends on Obama*, Reuters, December 30, 2009; *Do Airport Imagers Invade Privacy*, The San Francisco Chronicle, December 29, 2009; *No more getting naked for the TSA*, The Examiner, May 20, 2009; *X-Ray Body Scanner Stirs Controversy*, Fox Washington DC, May 18, 2009; *Airport scanners take 'naked' pics, group says*, CNN.com, Monday, May 18, 2009; Kai Jackson, *Total Body Scans At Airports Cause Controversy*, Channel 13 Baltimore, May 18, 2009; *Whole Body Imaging is Wholly Frightening*, Manolith.com, Monday, May 18, 2009; *Commentary: Whole-Body imaging invades privacy*, CNN.com, May 19, 2009; *Privacy Advocates Take Issue With 'Whole Body Imaging' Airport Security Technology*, All Headline News, May 19, 2009; *Airport scanners take 'naked' pics, group says*, CNN.com, Monday, May 18, 2009; *Airport body scans: An issue of privacy*, The Windsor Star (Canadian), Tuesday, May 12, 2009; Anice Tibbetts, *Airport officials make plans to conduct virtual strip searches*, CanWest News Service, May 6, 2009; David Copeland, *Scanner finds hidden objects, not flesh*, Boston.com, April 27, 2009; *Herald Poll: Porn at the airport?* Daily Herald, April 24, 2009; *Chaffetz wants ban on airport whole body imaging*, ABC Channel 4 (Salt Lake City), April 22, 2009; William Saletan, *Deeper Digital Penetration*, Slate, April 8, 2009; Sean O'Neill, *TSA: Whole-body scanners to replace metal detectors*, Budget Travel, April 7, 2009; Joe Sharkey, *Whole-Body Scans Pass First Airport Tests*, N.Y. Times, April 6, 2009; Jeremy Hsu, *Airport body scans reveal all*, MSNBC, Apr. 1, 2009; *New security scan at DFW Airport has privacy advocates worried*, Dallas Morning News, June 16, 2008; Thomas Frank, *TSA looks into using more airport body scans*, USA Today, October 7, 2007; William Saletan, *Digital Penetration*, Slate, Mar. 3, 2007; *Controversial X-ray machine to make national debut Friday at Sky Harbor*, Associate Press, February 21, 2007; *Phoenix Airport to Test X-Ray Screening*, Associate Press as reported on Privacy.org, December 1, 2006; Joe Sharkey, *Airport screeners could see X-rated X-Rays*, New York Times, May 24, 2005; Thomas Frank, *Airports roll out high-tech security*, USA Today, May 16, 2005; Ryan Single, *New Screening Technology Is Nigh*, Wired News, May 19, 2005; Bryon Okada, *TSA official says machine, not screeners, at fault*, Star-Telegram, May 1, 2005; Michael Grabell, *Airport plans to screen for explosives this fall Machines at D/FW*, Dallas News, May 1, 2005; Ryan Single, *Passenger Screening, Take 10*, Wired News, January 31, 2005; *'Nice Bombs Ya Got There'*, Associated Press, Wired News, June 26, 2003; Megan Lisagor, *TSA awards passenger screening contract*, Federal Computer Week, March 10, 2003; Megan Lisagor, *TSA prepares passenger screening system*, Federal Computer Week, February 26, 2003; *Smart Check-In Cuts Airport Lines*, Wired News, February 5, 2001.

As the sustained public interest concerning TSA's methods clearly attests, there is an "urgent need to inform the public" about this federal governmental activity. 6 C.F.R. § 5.5(d)(1)(ii).

2. ACLUM is an organization primarily engaged in disseminating information to inform the public.

ACLUM is an organization “primarily engaged in disseminating information” within the meaning of the FOIA statute and DHS regulations. 5 U.S.C. § 552(a)(6)(E)(v) (II); 6 C.F.R. § 5.5(d)(1)(ii). Obtaining information about government activity, analyzing that information, and widely publishing and disseminating that information to the press and public are critical and substantial components of ACLUM’s work and one of its primary missions. *See ACLU v. Dep’t of Justice*, 321 F. Supp. 2d 24, 30 n.5 (D.D.C. 2004) (finding non-profit public interest group that “gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw material into a distinct work, and distributes that work to an audience” to be “primarily engaged in disseminating information” (internal citation and quotation marks omitted)).⁵

ACLUM publishes newsletters, news briefings, reports and other printed materials that are disseminated to the public. *See* Exhibits A – C. ACLUM also disseminates information through its heavily subscribed website, www.aclum.org, a blog, <http://www.massrightsblog.org> and regular posts on social media sites such as Facebook and Twitter. *See* Exhibits D – F.

ACLUM regularly publishes reports about government activity and civil liberties issues based on its analysis of information derived from various sources, including information obtained from the government through FOIA. This material is broadly circulated to the public and widely available to everyone for no cost or, sometimes, for a small fee. Many ACLUM reports include a description and analysis of government documents obtained through FOIA.⁶

As the state affiliate of the national ACLU organization, ACLUM also disseminates information through the ACLU. Since 2007 alone, ACLU national projects have published and disseminated over 30 reports. The ACLU regularly publishes books, “know your rights” publications, fact sheets, and educational brochures and pamphlets designed to educate the public about civil liberties issues and government policies that implicate civil rights and liberties.⁷

⁵ Notably, courts have found organizations with missions similar to the ACLU and that engage in information dissemination activities similar to the ACLU to be “primarily engaged in disseminating information.” *See, e.g., Leadership Conference on Civil Rights v. Gonzales*, 404 F. Supp. 2d 246, 260 (D.D.C. 2005) (Leadership Conference on Civil Rights); *ACLU v. Dep’t of Justice*, 321 F. Supp. 2d at 30 n. 5 (Electronic Privacy Information Center).

⁶ *See e.g. Detention and Deportation in the Age of ICE*, available at www.aclum.org/ice and the accompanying document gallery of FOIA documents at <http://aclum.org/ice/gallery.php>.

⁷ A recent search of Amazon.com produced over 60 books published by the ACLU.

The ACLU operates a widely-read blog where original editorial content reporting on and analyzing civil rights and civil liberties news is posted daily.⁸ The ACLU also creates and disseminates original editorial and educational content on civil rights and civil liberties news through multi-media projects, including videos, podcasts, and interactive features.⁹ The ACLU has also produced an in-depth television series on civil liberties called “The Freedom Files.”¹⁰

The ACLU also publishes, analyzes, and disseminates information through its heavily visited website, www.aclu.org. The website addresses civil rights and civil liberties issues in depth, provides features on civil rights and civil liberties issues in the news, and contains many thousands of documents relating to the issues on which the ACLU is focused. The ACLU’s website also serves as a clearinghouse for news about ACLU cases, as well as analysis about case developments, and an archive of case-related documents. Through these pages, the ACLU also provides the public with educational material about the particular civil liberties issue or problem; recent news about the issue; analyses of Congressional or executive branch action on the issue; government documents obtained through FOIA about the issue; and more in-depth analytic and educational multi-media features on the issue.¹¹

The ACLU website includes many features on information obtained through the FOIA.¹² For example, the ACLU’s “Torture FOIA” webpage, <http://www.aclu.org/accountability/released.html>, contains commentary about the ACLU’s FOIA request, press releases, analysis of the FOIA documents, and an advanced search engine permitting webpage visitors to search the documents obtained through the FOIA, and advises that the ACLU in collaboration with Columbia University Press has published a book about the documents obtained through the FOIA.

⁸ See <http://www.aclu.org/blog>.

⁹ See <http://www.aclu.org/multimedia/index.html>.

¹⁰ See <http://aclu.tv/>.

¹¹ For example, the ACLU’s website about national security letter (“NSL”) cases, www.aclu.org/nsl, includes, among other things, an explanation of what NSLs are; information about and document repositories for the ACLU’s NSL cases, links to documents obtained through FOIA about various agencies’ use of NSLs; NSL news in the courts, Congress, and executive agencies; links to original blog posts commenting on and analyzing NSL-related news; educational web features about the NSL gag power; public education reports about NSLs and the Patriot Act; news about and analysis of the Department of Homeland Security Inspector General’s reviews of the FBI’s use of NSLs; the ACLU’s policy analysis and recommendations for reform of the NSL power; charts with analyzed data about the government’s use of NSL; myths and facts documents; and links to information and analysis of related issues.

¹² See, e.g., <http://www.aclu.org/accountability/released.html> (Torture FOIA) ; <http://www.aclu.org/accountability/olc.html> (OLC Memos); <http://www.aclu.org/national-security/csrt-foia> (CSRT FOIA); <http://www.aclu.org/national-security/aclu-v-doj-lawsuit-enforce-nsa-warrantless-surveillance-foia-request> (NSA FOIA); <http://www.aclu.org/national-security/patriot-foia> (Patriot Act FOIA); http://www.aclu.org/national-security_technology-and-liberty/spy-files (Spy Files).

The ACLU has also published a number of charts that collect, summarize, and analyze information it has obtained through FOIA. For example, through compilation and analysis of information gathered from various sources—including information obtained from the government through FOIA—the ACLU has created an original chart that provides the public and news media with a comprehensive index of Bush-era Office of Legal Counsel memos relating to interrogation, detention, rendition and surveillance which describes what is publicly known about the memos and their conclusions, who authored them and for whom, and whether the memos remain secret or have been released to the public in whole or in part.¹³ Similarly, the ACLU produced a chart of original statistics about the Defense Department’s use of National Security Letters based on its own analysis of records obtained through FOIA.¹⁴ Currently, the ACLU is producing a chart of documents regarding government surveillance obtained through FOIA and state public records requests around the country. The first chart in the series including d obtained by ACLUM in Massachusetts.¹⁵

Once released, ACLUM plans to make the information sought here available to the public through several formats, as it has done consistently with responses to FOIA requests in the past. Accordingly, expedited processing is appropriate in this case.

V. CONCLUSION

If our request is denied in whole or part, we ask that you justify all deletions by reference to specific exemptions of the FOIA and that you release all segregable portions of otherwise exempt material. We reserve the right to appeal a decision to withhold any information or to deny a waiver of fees or expedited processing.

We look forward to your reply to the Request within twenty (20) business days, as required under 5 U.S.C. § 552(a)(6)(A)(i). Please reply to this request to by contacting Laura Rótolo at the address above, (617) 482-3170 x311 or through email at lrotolo@aclum.org.

Thank you for your prompt attention to this matter.

Sincerely,

¹³ The chart is available at http://www.aclu.org/safefree/general/olcmemos_chart.pdf.

¹⁴ The chart is available at http://www.aclu.org/safefree/nationalsecurityletters/released/nsl_stats.pdf.

¹⁵ The chart is available at <http://www.aclu.org/spy-files-massachusetts>