2013

The D.C. Circuit's Epic Failure in *Electronic Privacy Information Center v. United States Department of Homeland Security*

R. Gregory Israelsen

Recommended Citation

R. Gregory Israelsen, *The D.C. Circuit's Epic Failure in Electronic Privacy Information Center v. United States Department of Homeland Security*, 78 J. AIR L. & COM. 711 (2013)
<https://scholar.smu.edu/jalc/vol78/iss4/1>

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Journal of Air Law and Commerce by an authorized administrator of SMU Scholar. For more information, please visit <http://digitalrepository.smu.edu>.

THE D.C. CIRCUIT’S EPIC FAILURE IN *ELECTRONIC
PRIVACY INFORMATION CENTER V. UNITED STATES
DEPARTMENT OF HOMELAND SECURITY*

R. GREGORY ISRAELSEN*

TABLE OF CONTENTS

I. INTRODUCTION..... 711

II. SIGNIFICANT LEGAL BACKGROUND 713

 A. *CITY OF INDIANAPOLIS V. EDMOND* 714

 B. *UNITED STATES V. HARTWELL* 715

III. FACTS AND PROCEDURAL HISTORY..... 716

 A. FACTS OF THE CASE..... 716

 B. PROCEDURAL HISTORY 718

IV. ANALYSIS..... 719

 A. OVERVIEW 719

 B. VIDEO VOYEURISM PREVENTION ACT..... 720

 C. PRIVACY ACT..... 724

 D. HOMELAND SECURITY ACT OF 2002 725

 E. RELIGIOUS FREEDOM RESTORATION ACT..... 726

 F. FOURTH AMENDMENT CLAIM 727

 G. THE COURT’S FLAWED CONCLUSION..... 734

V. CONCLUSION..... 736

I. INTRODUCTION

IN 2010, THE TRANSPORTATION Security Administration (TSA) implemented Advanced Imaging Technology (AIT) as the primary screening technology at airport security checkpoints across the United States.¹ A massive public backlash followed due to the perceived privacy violations associated with

* J.D., J. Reuben Clark Law School, Brigham Young University, 2013. The author would like to thank Professor Eric T. Jensen for his valuable guidance and insight on this article. Cory S. Clements also provided more assistance than any friend could hope for—the author is truly grateful.

¹ See *Advanced Imaging Technology (AIT)*, TSA, <http://www.tsa.gov/traveler-information/advanced-imaging-technology-ait> (last updated July 23, 2013).

AIT scanners.² For example, some feared that the use of body scanners would result in online “naked images” of the traveling public.³ Security experts disputed the security improvements offered by the scanners.⁴ A nationwide “opt-out” protest on the day before Thanksgiving 2010 threatened to significantly slow down travel times due to travelers opting for pat-downs instead of body scans.⁵ The discomfort that some passengers felt about enhanced pat-downs⁶ became infamous when one traveler warned a TSA screener, “If you touch my junk, I’ll have you arrested.”⁷

The issue of the legality of body scanners eventually made its way through the courts and was reviewed by the U.S. Court of Appeals for the District of Columbia (D.C. Circuit). The Electronic Privacy Information Center, along with several other named plaintiffs, brought a complaint against the TSA for violations of multiple statutes, as well as the Fourth Amendment, in

² But cf. Marc Ambinder, *White House Fights Pat-Down Backlash*, NAT’L J. (Nov. 22, 2010), <http://www.nationaljournal.com/whitehouse/white-house-fights-pat-down-backlash-20101122> (“[The White House] also disputed the very notion of a public backlash.”).

³ Joel Johnson, *One Hundred Naked Citizens: One Hundred Leaked Body Scans*, GIZMODO (Nov. 16, 2010), <http://gizmodo.com/5690749/these-are-the-first-100-leaked-body-scans> (revealing that 100 scans from a Florida courthouse were released in response to a Freedom of Information Act request).

⁴ Bruce Schneier, *A Waste of Money and Time*, N.Y. TIMES (Oct. 17, 2012), <http://www.nytimes.com/roomfordebate/2010/11/22/do-body-scanners-make-us-safer/a-waste-of-money-and-time>.

⁵ See Say “I Opt Out” of Naked-Body Scanners on National Opt Out Day, November 24, WE WON’T FLY, <http://wewontfly.com/opt-out-day/> (last visited April 24, 2013). Note that many airports simply used magnetometers instead of body scanners to prevent protest-caused delays. E.g., *Newark Airport Controversial Scanners Are Barely Used on Busiest Travel Day*, N.J. STAR LEDGER (Nov. 25, 2010), http://www.nj.com/news/index.ssf/2010/11/newark_liberty_airport_controv.html (“The majority of Newark’s full-body scanners were idle throughout much of the day, depriving most passengers of the chance to opt out of the controversial screening procedure even if they had wanted to.”).

⁶ Jeffrey Goldberg, *For the First Time, the TSA Meets Resistance*, ATLANTIC (Oct. 29, 2010), <http://www.theatlantic.com/national/archive/2010/10/for-the-first-time-the-tsa-meets-resistance/65390/> (describing “[a] journey through the security line at the Baltimore airport”).

⁷ Matthew Kaminski, *In Defense of Scanners and Pat-Downs*, WALL ST. J. (Dec. 4, 2010), <http://online.wsj.com/article/SB10001424052748703989004575652651928049266.html>; see also *Man to Security: Don’t “Touch My Junk”*, YOUTUBE (Nov. 15, 2010), <http://www.youtube.com/watch?v=R24DyuoZLaM>; Charles Krauthammer, *Don’t Touch My Junk*, WASH. POST (Nov. 19, 2010), <http://www.washingtonpost.com/wp-dyn/content/article/2010/11/18/AR2010111804494.html>.

connection with the TSA's rollout of AIT devices.⁸ This article critiques the D.C. Circuit's short opinion. The court held that while the TSA had failed to properly engage in notice-and-comment proceedings before implementing AIT scanners, the use of AIT scanners did not violate the other claimed statutes or the Constitution.⁹

The D.C. Circuit's analysis of the statutory and constitutional issues surrounding AIT scanners was too abbreviated and based on overly attenuated case law or simply faulty logic. This article does not argue whether the court came to the correct conclusion, but instead examines the court's flawed analysis. The D.C. Circuit's ruling in *Electronic Privacy Information Center v. U.S. Department of Homeland Security (EPIC)*¹⁰ was so flawed that no future court should rely on it as precedent—especially as an issue of first impression.

II. SIGNIFICANT LEGAL BACKGROUND

The Supreme Court has never considered the question of body scanners at airport security checkpoints. It has, however, ruled on several privacy-related cases in the past few terms. Most of these cases have generally been favorable to privacy advocates, even if that privacy comes at the expense of the government's interest in maintaining safety or public order.¹¹

Several other circuits have considered various post-September 11, 2001 (9/11) airport security measures, such as requiring identification at security,¹² x-raying carry-on baggage,¹³ and con-

⁸ *Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 653 F.3d 1, 2–3 (D.C. Cir. 2011).

⁹ *Id.* at 8–11.

¹⁰ *Id.* at 1.

¹¹ See *Missouri v. McNeely*, 133 S. Ct. 1552 (2013) (holding that the Fourth Amendment protects persons against a rule that always allows warrantless blood draws in DUI cases); *Florida v. Jardines*, 133 S. Ct. 1409 (2013) (holding that the Fourth Amendment protects against police using a drug-sniffing dog in the curtilage of a home without a warrant); *United States v. Jones*, 132 S. Ct. 945 (2012) (holding that the Fourth Amendment protects against the police using a GPS vehicular tracking device without a warrant); *Kyllo v. United States*, 533 U.S. 27 (2001) (holding that the Fourth Amendment protects against police use of a thermal-imager on a home without a warrant). Other circuits have similarly upheld Fourth Amendment privacy claims, even in the face of compelling government interests. *E.g.*, *United States v. Cotterman*, 709 F.3d 952, 963 (9th Cir. 2013) (holding that the Fourth Amendment prevents a border patrol agent from investigating a computer's files without a warrant).

¹² See *Gilmore v. Gonzales*, 435 F.3d 1125, 1129 (9th Cir. 2006).

¹³ See *United States v. Aukai*, 497 F.3d 955, 961 (9th Cir. 2007).

ducting increasingly invasive searches of individuals who failed a less invasive search.¹⁴ The D.C. Circuit in *EPIC* relied on several cases when analyzing airport security searches using the administrative-search exception.¹⁵ To assist in analyzing the court's reading of those cases, this article briefly summarizes those cases below.

A. *CITY OF INDIANAPOLIS V. EDMOND*

The D.C. Circuit relied on *City of Indianapolis v. Edmond*¹⁶ for the proposition that the "need to search airline passengers 'to ensure public safety can be particularly acute.'"¹⁷ In *Edmond*, the Supreme Court held that city police drug-interdiction checkpoints violated the Fourth Amendment.¹⁸ The Court explained that "[t]he Fourth Amendment requires that searches and seizures be reasonable."¹⁹ The Court also noted that it has "allowed searches for certain administrative purposes without particularized suspicion of misconduct, provided that those searches are appropriately limited."²⁰ But generally speaking, the Court has "never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing."²¹

Instead, the Court has only approved of checkpoint programs that are "designed primarily to serve purposes closely related to the problems of policing the border or the necessity of ensuring roadway safety."²² In determining the constitutionality of a particular program, the Court scrutinizes the type of public interest that the program is meant to serve.²³ Furthermore, "the gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose."²⁴

Of particular interest to courts analyzing airport security searches after *Edmond* is the Court's note that its holding—that

¹⁴ See *id.* at 962.

¹⁵ *Elec. Privacy Info. Ctr.*, 653 F.3d at 8–11.

¹⁶ 531 U.S. 32 (2000).

¹⁷ *Elec. Privacy Info. Ctr.*, 653 F.3d at 10 (quoting *Edmond*, 531 U.S. at 48).

¹⁸ *Edmond*, 531 U.S. at 48.

¹⁹ *Id.* at 37.

²⁰ *Id.*

²¹ *Id.* at 41.

²² *Id.*

²³ *Id.* at 43 (stating that the Court "must look more closely at the nature of the public interests that such a regime is designed principally to serve").

²⁴ *Id.* at 42.

certain drug checkpoints violate the Fourth Amendment—"does not affect the validity of border searches or searches at places like airports . . . where the need for such measures to ensure public safety can be particularly acute."²⁵

B. *UNITED STATES V. HARTWELL*

The plaintiffs in *EPIC* cited *United States v. Hartwell*²⁶ as persuasive precedent for how the court ought to analyze an airport search using the administrative-search exception.²⁷ In *Hartwell*, the Third Circuit held that the search of a defendant at an airport checkpoint was justified under the administrative-search doctrine.²⁸ Christian Hartwell set off a metal detector at the Philadelphia International Airport in May 2003.²⁹ A TSA agent then used a magnetic wand to perform a more pointed scan of Mr. Hartwell's person.³⁰ After detecting something in Hartwell's pocket, the agent discovered that Hartwell's pocket contained drugs, and Hartwell was arrested.³¹

Applying the test for administrative searches established by the Supreme Court in *Brown v. Texas*,³² the Third Circuit held that the TSA agent's search of Hartwell was permissible under the Fourth Amendment.³³ "Suspicionless checkpoint searches are permissible under the Fourth Amendment when a court finds a favorable balance between 'the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty.'"³⁴

To meet the first *Brown* factor, the court noted that "there can be no doubt that preventing terrorist attacks on airplanes is of paramount importance."³⁵ Undoubtedly, there is voluminous ev-

²⁵ *Id.* at 47–48.

²⁶ 436 F.3d 174 (3d Cir. 2006). *Hartwell* was authored by current Supreme Court Justice Samuel Alito before his appointment to the U.S. Supreme Court.

²⁷ *Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 653 F.3d 1, 10–11 (D.C. Cir. 2011).

²⁸ *Hartwell*, 436 F.3d at 177.

²⁹ *Id.* at 175.

³⁰ *Id.*

³¹ *Id.* at 176.

³² 443 U.S. 47, 51 (1979). The three factors established in *Brown* include (1) "a weighing of the gravity of the public concerns served by the seizure"; (2) "the degree to which the seizure advances the public interest"; and (3) "the severity of the interference with individual liberty." *Id.* at 50–51.

³³ *Hartwell*, 436 F.3d at 177.

³⁴ *Id.* at 178–79 (quoting *Illinois v. Lidster*, 540 U.S. 419, 427 (2004)).

³⁵ *Id.* at 179.

idence and support for the government's actions taken to ensure safe air travel.³⁶

With respect to the second factor, the court held that *Brown* requires that airport checkpoints "advance the public interest."³⁷ The court pointed out that a pre-boarding search is the only effective way to detect airline passengers who "'are reasonably likely to hijack an airplane.'"³⁸ And because there is no way to know which passengers are potential hijackers, it follows that all passengers must be searched.³⁹ But the court was also careful to say that screening procedures "'have every indicia of being the most efficacious that could be used'" and that "airport checkpoints have been effective."⁴⁰

The court held that "the procedures involved in Hartwell's search were minimally intrusive, . . . well-tailored to protect personal privacy, escalating in invasiveness only after a lower level of screening disclosed a reason to conduct a more probing search," and therefore met the third *Brown* factor.⁴¹ Furthermore, the first several searches "involved no physical touching"—they were instead "less intrusive substitute[s] for a physical pat-down."⁴²

III. FACTS AND PROCEDURAL HISTORY

A. FACTS OF THE CASE

The events on 9/11 changed the face of air travel forever. Multiple armed terrorists hijacked several airplanes and used them as missiles to attack the World Trade Center in New York, New York, and the Pentagon in Washington, D.C.⁴³ Another hijacked plane crashed in Pennsylvania.⁴⁴ In response, America in-

³⁶ See *id.*

³⁷ *Id.*

³⁸ *Id.* at 180 (quoting *Singleton v. Comm'r*, 606 F.2d 50, 52 (3d Cir. 1979)).

³⁹ *Id.*

⁴⁰ *Id.* (quoting *United States v. Skipwith*, 482 F.2d 1272, 1275 (5th Cir. 1973)).

⁴¹ *Id.* Note that the court included a footnote pointing out that it was not "set[ting] the outer limits of intrusiveness in the airport context," nor was it "devis[ing] any bright-line test to implement the Brown standard in all future cases." *Id.* at n.10. It was merely "hold[ing] that Hartwell's search was 'minimally intrusive' under *Brown*." *Id.*; see *infra* note 144 and accompanying text.

⁴² *Hartwell*, 436 F.3d at 180.

⁴³ *9/11 and TSA*, TSA (Sept. 11, 2013), <http://www.tsa.gov/about-tsa/911-and-tsa>.

⁴⁴ *Id.*

initiated wars on multiple fronts, eventually finding and killing most of those responsible for planning the attacks.⁴⁵

The 9/11 attacks also fundamentally changed the experience of air travel generally and airport security specifically. Congress created the TSA in response to the 9/11 attacks; the TSA eventually became part of the new Department of Homeland Security.⁴⁶ Since 2001, the TSA has continuously implemented new security measures in response to different terrorist plots discovered by intelligence sources.⁴⁷ For example, the TSA purchased and began using body scanners at airports nationwide in response to “underwear bomber” Umar Farouk Abdulmutallab’s attempt to detonate plastic explosives sewn into his underwear while on board Northwest Airlines Flight 253 from Amsterdam to Detroit, Michigan.⁴⁸

In 2007, the TSA began testing AIT to enable detection of explosives and other non-metal threats to aviation security.⁴⁹ Two types of technology have been developed and used in airports: “millimeter wave and backscatter. Millimeter wave technology bounces electromagnetic waves off the body to create a black and white three-dimensional image. Backscatter technology projects low level X-ray beams over the body to create a reflection of the body displayed on the monitor.”⁵⁰

⁴⁵ Katrina vanden Heuvel, *With Osama bin Laden Dead, It's Time to End the "War on Terror"*, NATION (May 2, 2011), <http://www.thenation.com/blog/160310/osama-bin-laden-dead-its-time-end-war-terror>.

⁴⁶ 9/11 and TSA, *supra* note 43.

⁴⁷ Richard Reid—the “shoe bomber”—led to travelers having to remove their shoes. Pam Belluck & Kenneth Chang, *A Nation Challenged: The Investigation: Shoes Were a “Homemade Bomb,” F.B.I. Agent Says*, N.Y. TIMES (Dec. 29, 2001), <http://www.nytimes.com/2001/12/29/us/a-nation-challenged-the-investigation-shoes-were-a-homemade-bomb-fbi-agent-says.html>. A plot to use liquid explosives to blow up flights from Britain to America led to banning liquids completely; this rule was later changed to permit liquids in restricted amounts. Alan Cowell & Dexter Filkins, *Terror Plot Foiled; Airports Quickly Clamp Down*, N.Y. TIMES (Aug. 11, 2006), <http://www.nytimes.com/2006/08/11/world/europe/11plot.html>. Umar Farouk Abdulmutallab—the “underwear bomber”—led to body scanners. Joe Sharkey, *Annoyances Mount over the Body Scanner*, N.Y. TIMES (July 19, 2010), <http://www.nytimes.com/2010/07/20/business/20road.html>.

⁴⁸ Kenneth Chang, *Explosive on Flight 253 Is Among Most Powerful*, N.Y. TIMES (Dec. 27, 2009), www.nytimes.com/2009/12/28/us/28explosives.html.

⁴⁹ OFFICE OF INSPECTOR GEN., U.S. DEP’T OF HOMELAND SEC., OIG No. 12-06, TSA PENETRATION TESTING OF ADVANCED IMAGING TECHNOLOGY (Nov. 2011), www.oig.dhs.gov/assets/Mgmt/OIG_SLR_12-06_Nov11.pdf [hereinafter TSA PENETRATION TESTING].

⁵⁰ *Id.*

The TSA responded to Abdulmutallab's 2009 bombing attempt, as mentioned above, by beginning to use body scanners as the primary screening method at airport security checkpoints nationwide.⁵¹ TSA policy mandates that after a passenger has passed through the scanner and has been cleared, the image is deleted.⁵² The TSA screener can neither save the image nor bring a camera or cell phone into the image-viewing room.⁵³

Travelers are not required to submit to a body scan, but if they "opt-out," they are required to receive an "enhanced pat-down"—a pat-down that was changed in tandem with the body scanner rollout to implement stricter security protocols, including touching sensitive areas.⁵⁴

In 2012, Congress passed the FAA Modernization and Reform Act,⁵⁵ which, among other things, requires the use of Automated Target Recognition technology—which uses a generic passenger image and automatically identifies any areas for additional screening⁵⁶—for all passenger screening beginning June 1, 2012.⁵⁷ The TSA announced in January 2013 that it would remove all remaining backscatter-imaging scanners from airports by June 1, 2013, but leave in place millimeter-wave scanners using Automated Target Recognition software.⁵⁸

B. PROCEDURAL HISTORY

In 2009, more than thirty organizations—one of which was plaintiff EPIC—wrote to the Secretary of Homeland Security, objecting to the TSA's use of body scanners as the primary screening method at U.S. airports.⁵⁹ They requested that the

⁵¹ *Id.*

⁵² *Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 653 F.3d 1, 4 (D.C. Cir. 2011).

⁵³ *Id.* Note that there is only an image-viewing room for backscatter-imaging scanners because these machines use actual passenger images instead of generic passenger outlines to identify passengers that need additional screening.

⁵⁴ *Id.* at 3.

⁵⁵ FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 826, 126 Stat. 11, 132–33 (codified at 49 U.S.C. § 44901(1)).

⁵⁶ Automated Target Recognition technology removes the need for a TSA employee to sit in a separate room because scan results do not display passenger-specific images; they only show a generic outline with potential problem areas marked. TSA PENETRATION TESTING, *supra* note 49.

⁵⁷ FAA Modernization and Reform Act of 2012 § 826.

⁵⁸ Ron Nixon, *Unpopular Full-Body Scanners to Be Removed from Airports*, N.Y. TIMES (Jan. 18, 2013), <http://www.nytimes.com/2013/01/19/us/tsa-to-remove-invasive-body-scanners.html>.

⁵⁹ *Elec. Privacy Info. Ctr.*, 653 F.3d at 4.

TSA stop using body scanners and engage in a “90-day formal public rulemaking process.”⁶⁰ The TSA ignored this request for formal rulemaking, but it did respond with a letter addressing the organizations’ substantive concerns.⁶¹

In 2010, EPIC and another group sent a second letter requesting “the issuance, amendment, or repeal of a rule” about body scanners.⁶² They claimed that the use of body scanners violates the Privacy Act, the Religious Freedom Restoration Act, and the Fourth Amendment, and that the TSA needed to prepare a privacy impact assessment before issuing the new rule mandating the use of body scanners as the primary screening technology.⁶³ The TSA responded by taking the position that it is not required to initiate rulemaking to change screening procedures.⁶⁴ In July 2010, two individuals joined EPIC in petitioning the D.C. Circuit for review.⁶⁵

The D.C. Circuit held that the TSA had no justification for its failure to conduct a notice-and-comment rulemaking.⁶⁶ The court remanded to the agency for further proceedings but did not vacate the rule—i.e., it did not disallow the use of body scanners—“[b]ecause vacating the present rule would severely disrupt an essential security operation . . . and the rule is . . . otherwise lawful.”⁶⁷ The court then proceeded to dismiss all the substantive claims—both statutory and constitutional—against the use of body scanners.⁶⁸

IV. ANALYSIS

A. OVERVIEW

This article does not address whether the D.C. Circuit came to the right conclusion with regard to the legality—under federal statutes or the Fourth Amendment—of the TSA’s use of body scanners to screen U.S. airline passengers.⁶⁹ Instead, this article

⁶⁰ *Id.*

⁶¹ *Id.*

⁶² *Id.*

⁶³ *Id.*

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ *Id.* at 8.

⁶⁷ *Id.*

⁶⁸ *Id.* at 8–11.

⁶⁹ *Id.* at 2–3. There are many other scholarly articles that argue the merits of whether as a statutory or constitutional issue AIT devices should be allowed as primary screening technology in U.S. airports. See Jennifer S. Ellison & Marc

analyzes the D.C. Circuit's flawed opinion in *EPIC* and argues that the D.C. Circuit's reasoning is so flawed that it should not be used as precedent in other judicial decisions.

Professor Akhil Reed Amar's statement regarding the Supreme Court has equal import when applied to a circuit court: "[E]ven when the modern Court has reached sound results, it has often given suspect reasons."⁷⁰ Such is the case here. The D.C. Circuit failed to adequately address the legal questions surrounding the plaintiffs' claims. This failure to "say what the law is"⁷¹ is particularly troubling given the fact that this case was the first—and only—time that an appellate court has considered many of the questions surrounding the TSA's nationwide use of body scanners.⁷²

The plaintiffs' substantive claims against the use of body scanners included four statutory claims and a Fourth Amendment claim.⁷³ The D.C. Circuit's shortcomings in adequately resolving the legal questions raised by each alleged violation are treated in turn.

B. VIDEO VOYEURISM PREVENTION ACT

The first statutory claim against the use of AIT scanners as the primary screening technology was that AIT screening violates the Video Voyeurism Protection Act.⁷⁴ The Video Voyeurism Protection Act was passed in 2004 to combat the threat of technology "to the privacy of unsuspecting adults" and especially to

Pilcher, *Advanced Imaging Technology (AIT) Deployment: Legal Challenges and Responses*, 24 AIR & SPACE LAW. 4 (2012) (arguing that AIT scanners pose no problem); Brittany R. Stancombe, *Fed Up with Being Felt Up: The Complicated Relationship Between the Fourth Amendment and TSA's "Body Scanners" and "Pat-Downs"*, 42 CUMB. L. REV. 181 (2012) (arguing that AIT scanners violate the Fourth Amendment).

⁷⁰ Akhil Reed Amar, *Foreword: The Document and the Doctrine*, 114 HARV. L. REV. 26, 75 (2000).

⁷¹ See *Marbury v. Madison*, 5 U.S. 137, 177 (1803).

⁷² Notably, the Supreme Court has never taken up the issue. See Jeffrey Rosen, *"Don't Touch My Junk" Sneaks into the Supreme Court*, NEW REPUBLIC (Nov. 1, 2012), <http://www.newrepublic.com/blog/plank/109463/dont-touch-my-junk-sneaks-the-supreme-court>.

⁷³ The statutory claims against the use of AIT scanners as primary screening technology included claims under the Video Voyeurism Protection Act, under the Privacy Act, that the Department of Homeland Security's Chief Privacy Officer failed to discharge her statutory duties with regard to technology and privacy protections, and under the Religious Freedom Restoration Act. *Elec. Privacy Info. Ctr.*, 653 F.3d at 8.

⁷⁴ 18 U.S.C. § 1801 (2012).

offer "protections for individuals who may be photographed in compromising positions in public places."⁷⁵

The TSA made two arguments in response to the claim. First, it argued that the plaintiffs could not rightly bring the claim "because it was not raised before the agency."⁷⁶ But, the plaintiffs argued, there was no TSA proceeding in which they could have even raised the argument.⁷⁷ The court did not comment on this argument other than to correctly point out that the "absence of [a TSA proceeding] is the very matter at issue here."⁷⁸

The TSA's second argument was that in any case, the Video Voyeurism Protection Act provides an exception—Section 1801(c)—for "any lawful law enforcement, correctional, or intelligence activity," which means that TSA screeners cannot be liable under Section 1801.⁷⁹ The plaintiffs argued both that the alleged Fourth Amendment violation meant that the scans were not lawful activity and that "the TSA does not engage in 'law enforcement, correctional, or intelligence activity.'"⁸⁰ Because the court rejected the Fourth Amendment claim,⁸¹ it ignored the plaintiffs' unlawful activity argument. The court also dismissed the law enforcement argument with a laugh, only saying that it "borders upon the silly."⁸²

In fact, Section 1801 does not provide a definition for any of the terms used in Section 1801(c).⁸³ There is no precedent in case law for applying the law enforcement exception, meaning that the D.C. Circuit was—as in many parts of its opinion—establishing new precedent. The court summarily declared the plaintiffs' argument to be "silly," but in fact the plaintiffs were quite serious.⁸⁴ A reasonable court could easily hold that TSA screening operations do not fall under any of the established categories of Section 1801's exception: law enforcement, correctional, or intelligence activity.

⁷⁵ H.R. REP. NO. 108-504, at 2–3 (2004), *reprinted in* 2004 U.S.C.C.A.N. 3292 (explaining the need for the Video Voyeurism Protection Act).

⁷⁶ *Elec. Privacy Info. Ctr.*, 653 F.3d at 8.

⁷⁷ *Id.*

⁷⁸ *Id.*

⁷⁹ *See* 18 U.S.C. § 1801.

⁸⁰ *Elec. Privacy Info. Ctr.*, 653 F.3d at 8.

⁸¹ *See infra* Part IV.F.

⁸² *Elec. Privacy Info. Ctr.*, 653 F.3d at 8.

⁸³ The section defines: "capture," "broadcast," "a private area of the individual," "female breast," and "under circumstances in which that individual has a reasonable expectation of privacy." 18 U.S.C. § 1801(b).

⁸⁴ *Elec. Privacy Info. Ctr.*, 653 F.3d at 8.

First, TSA screening operations do *not* constitute law enforcement activity.⁸⁵ The law specifically establishes that screening operations are “carried out by a Federal Government Employee.”⁸⁶ Many court opinions also acknowledge that TSA screening procedures are not the equivalent of law enforcement activity.⁸⁷ Granted, the text of Section 1801’s exception may arguably be read to reach more broadly than simply encompassing law enforcement officers.⁸⁸ That is, “law enforcement activity” might be performed by someone other than a police officer or other law enforcement agent.⁸⁹ But such a reading would be unreasonable because then nearly any government action could be construed as “law enforcement activity.” Put another way, the fact that a government employee does her job in accordance with the law does not automatically mean she is engaged in “law enforcement activity.” Under such a broad reading, for example, a mailman delivering the mail could be said to be engaged in “law enforcement activity” because he is enforcing the mail delivery law⁹⁰ by delivering the mail.⁹¹ Another reason that “law enforcement activity” cannot be read so broadly as to include

⁸⁵ Note that the TSA does have an Office of Law Enforcement—it administers the Federal Air Marshal service. See *Office of Law Enforcement*, TSA, <http://www.tsa.gov/about-tsa/office-law-enforcement> (last updated May 9, 2013). But airport screening agents, in contrast to Federal Air Marshals, are not federal law enforcement officers.

⁸⁶ 49 U.S.C. § 44901(a) (2006). “Federal Government Employee” is defined in 5 U.S.C. § 2105; nothing in that definition can be read to include “law enforcement, correctional, or intelligence activity.” See *id.*

⁸⁷ See, e.g., *United States v. McCarty*, 648 F.3d 820, 825 (9th Cir. 2011) (describing TSA Operations Direction OD-400-54-2, which requires a TSA screener “to call a law enforcement officer” to investigate if she finds contraband). It would not make sense to require a TSA screener to call for a law enforcement officer if the TSA screener herself was engaged in law enforcement.

⁸⁸ This relies on the idea that law enforcement activity may be performed by non-law enforcement officers.

⁸⁹ *But cf.* *Mich. Dep’t of State Police v. Sitz*, 496 U.S. 444, 453 (1990) (noting that the checkpoint search performed by “uniformed police officers” factored into the Fourth Amendment analysis because it lessened the intrusion); *City of Indianapolis v. Edmond*, 531 U.S. 32, 42 (2000) (noting that “[s]ecuring the border and apprehending drunk drivers are, of course, law enforcement activities, and law enforcement officers employ arrests and criminal prosecutions in pursuit of these goals” (emphasis added)).

⁹⁰ See 39 U.S.C. § 403 (2006).

⁹¹ Under this reading, almost any federal government employee could be involved in law enforcement activity. As another example, a toll-booth collector ensures that people follow the toll-related laws before driving on toll roads. In the same way, airport screeners ensure that people follow carry-on baggage laws before flying on an airplane.

any government employee following the law is that such a reading would render the rest of the exception meaningless—that is, correctional and intelligence activity. The courts give meaning to each word of a statute.⁹² Therefore, “law enforcement activity” should be construed narrowly to include activity engaged in by law enforcement officers, a statutorily defined group that does not include TSA screening agents.

Second, TSA airport screening procedures are not “correctional activity.” Correctional activity, according to its plain text meaning,⁹³ applies to correctional officers and activity taking place at correctional facilities—*e.g.*, prisons—not airports.

Third, TSA screening operations are not “intelligence activity.”⁹⁴ The Aviation and Transportation Security Act directs the TSA to act “as the primary liaison for transportation security to the intelligence and law enforcement communities.”⁹⁵ The TSA must perform something other than “intelligence and law enforcement” activity if the TSA is to be a liaison to the intelligence and law enforcement communities.⁹⁶ While the TSA does maintain its own small Office of Intelligence—in 2006, it included about 139 people—airport screeners do not engage in intelligence activity.⁹⁷ Airport screeners seek “to deter and physically prevent terrorists from carrying out a planned attack”; in

⁹² *E.g.*, *Duncan v. Walker*, 533 U.S. 167, 175 (2001) (“[This Court has the] duty to give effect, if possible, to every clause and word of a statute.”); *see also* *Murphy Exploration & Prod. Co. v. U.S. Dep’t of the Interior*, 252 F.3d 473, 481 (D.C. Cir. 2001) (It is an “‘endlessly reiterated principle of statutory construction . . . that all words in a statute are to be assigned meaning, and that nothing therein is to be construed as surplusage.’” (quoting *Qi-Zhuo v. Meissner*, 70 F.3d 136, 139 (D.C. Cir. 1995))).

⁹³ *See* *Conn. Nat’l Bank v. Germain*, 503 U.S. 249, 254 (1992) (“When the words of a statute are unambiguous, then, this first canon is also the last: ‘judicial inquiry is complete.’”).

⁹⁴ But, as noted earlier, the court actually found none of these—it dismissed the argument as “silly.” *Elec. Privacy Info. Ctr. v. U.S. Dep’t of Homeland Sec.*, 653 F.3d 1, 8 (D.C. Cir. 2011).

⁹⁵ 49 U.S.C. § 114(f)(5) (2006).

⁹⁶ “Liaison” is defined as “a person who acts as a link to assist communication or cooperation between groups of people.” *Definition of Liaison in English*, OXFORD DICTIONARIES, http://www.oxforddictionaries.com/us/definition/american_english/liaison (last visited Nov. 24, 2013).

⁹⁷ *Transp. Sec. Admin.’s Office of Intelligence: Hearing Before the Subcomm. on Intelligence, Info. Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 109th Cong. 5 (2006) (statement of William Gaches, Assistant Adm’r for Intelligence, Transp. Sec. Admin.) (“The intelligence office at TSA is comprised of 99 government personnel and about 40 contractors.”).

contrast, the Office of Intelligence seeks to “stop[] terrorists before they launch an attack.”⁹⁸

There may be a valid argument that airport security operations are “law enforcement, correctional, or intelligence activity,”⁹⁹ as is required for the exception to apply.¹⁰⁰ But a plain reading of the law denies the TSA the exception.¹⁰¹

Even if the court could have properly found that TSA screening is law enforcement or intelligence activity, the court failed in its duty to draw the required connection between the law and the facts; the court failed to explain how TSA screening could fall into the Video Voyeurism Prevention Act’s exception. The court’s summary dismissal of the plaintiffs’ claim under the Act as “silly”¹⁰² constituted a complete abandonment of the court’s responsibility to provide insight both to the parties before it and to similarly situated parties in future cases by justifying its holding using sound methods of reasoning. Particularly because no other court has construed the application or reach of Section 1801(c) in any context—not just the airport security context—the D.C. Circuit’s failure to address the real legal questions validly before it is especially unsettling.

C. PRIVACY ACT

The plaintiffs’ next claim against the use of AIT as the primary screening method was that it violated the Privacy Act of

⁹⁸ *Id.*

⁹⁹ 18 U.S.C. § 1801(c) (2006).

¹⁰⁰ For example, the D.C. Circuit might have looked to factors other than case law, such as legislative history or intent. Maybe the court considered such other factors but simply omitted them from the opinion. Note that even if such an argument *could* be made, the D.C. Circuit did not do so. The court might have argued that TSA screening operations support intelligence by providing intelligence officers with information relating to the types of threats actually faced at airport security checkpoints. One flaw of such an argument is the slippery slope that it quickly leads to. If federal government employees—such as TSA screening officers—are not subject to Section 1801(c) because they might provide intelligence officers with useful intelligence, then there is almost no federal government employee that does not meet the exception, as doubtless almost any public position could potentially produce data that is eventually used by an intelligence officer conducting intelligence work. See note 91, *supra*, for a similar discussion of the same slippery slope associated with considering TSA screeners to be engaged in law enforcement activity.

¹⁰¹ As shown in this section, TSA screening activities do not fall under the statutorily defined categories of law enforcement, correctional, or intelligence activity.

¹⁰² *Elec. Privacy Info. Ctr. v. U.S. Dep’t of Homeland Sec.*, 653 F.3d 1, 8 (D.C. Cir. 2011).

1974 (Privacy Act).¹⁰³ The court rejected the Privacy Act claim in part because the plaintiffs did not offer any reason to believe that the TSA had in fact combined various sources of information and then linked names to the images produced using AIT.¹⁰⁴ But in reality, no plaintiff could ever meet that standard. "[T]he presumptions for the government and the exceptions built into the Freedom of Information Act" make it "almost impossible for a plaintiff to engage in discovery and successfully sue a defense agency for a Privacy Act violation."¹⁰⁵

Thus, it is possible that the D.C. Circuit had no choice but to fail to provide any meaningful guidance for future litigants of Privacy Act claims. Instead, the solution may lie with Congress; the legislature could revise either the Privacy Act or the Freedom of Information Act to allow courts access to the information that they and plaintiffs need to determine whether a Privacy Act violation has actually occurred.¹⁰⁶

D. HOMELAND SECURITY ACT OF 2002

Another statutory claim against the body scanner rollout was that the Department of Homeland Security's Chief Privacy Officer failed to discharge her statutory duties to assure that the use of technologies does not erode privacy protections and to make an assessment of the rule's impact upon privacy.¹⁰⁷ Congress created the Chief Privacy Officer position to ensure that Department of Homeland Security activities are conscientious and protective of privacy.¹⁰⁸ One of the Chief Privacy Officer's responsibilities is to "conduct . . . a privacy impact assessment of proposed rules of the Department . . . on the privacy of personal information, including the type of personal information collected and the number of people affected."¹⁰⁹

¹⁰³ Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552(a) (2012)); *Elec. Privacy Info. Ctr.*, 653 F.3d at 4.

¹⁰⁴ *Elec. Privacy Info. Ctr.*, 653 F.3d at 8.

¹⁰⁵ David Gusella, *Violating Privacy in Private: How EPIC v. DHS Creates an Impossible Burden on Plaintiffs Trying to Demonstrate a Privacy Act Violation*, 53 B.C.L. REV. E-SUPP. 169, 170 (2012). This article does not go into great detail on the court's flaws with respect to the Privacy Act claim because other scholarly work has already done so. *E.g., id.*

¹⁰⁶ The Privacy Act cannot protect privacy if the courts do not have access to the information they need to determine whether a privacy violation has occurred.

¹⁰⁷ *Elec. Privacy Info. Ctr.*, 653 F.3d at 8–9.

¹⁰⁸ See 6 U.S.C. § 142 (2012).

¹⁰⁹ *Id.* § 142(a)(4).

The D.C. Circuit's short paragraph about the privacy impact assessment is illogical and confusing. First, the court infers that the Chief Privacy Officer's failure to make an assessment was actually an affirmative determination that her prior efforts to assess the privacy impact of using body scanners generally were good enough to cover the privacy impact of using body scanners as the primary screening technology.¹¹⁰ The Chief Privacy Officer's failure to act, however, is not the same as an affirmative determination; her failure to act means only that she did not act. In other words, not making a determination is different from making a negative determination. The court's logical error here is relevant precisely because the Chief Privacy Officer had an affirmative duty to make that very same privacy determination.¹¹¹

Second, the court's conclusions regarding the notice-and-comment proceedings create a further conflict when compared to its conclusions about the Chief Privacy Officer's privacy assessment. When finding that the TSA should have engaged in a notice-and-comment proceeding before making body scanners the primary screening method at airports nationwide, the court explicitly recognized that the expansion of body scanners represented a distinctly different and potentially problematic privacy concern.¹¹² But that creates a conflict within the court's opinion—the court claims that body scanners represent a difference in kind that requires notice-and-comment proceedings but also implicitly claims that body scanners do not require a privacy impact analysis because they do not represent a difference in kind from previous privacy impact assessments.¹¹³

E. RELIGIOUS FREEDOM RESTORATION ACT

The D.C. Circuit properly dismissed the plaintiffs' claims under the Religious Freedom Restoration Act (RFRA) for lack

¹¹⁰ See *Elec. Privacy Info. Ctr.*, 653 F.3d at 9.

¹¹¹ 6 U.S.C. § 142(a)(4).

¹¹² *Elec. Privacy Info. Ctr.*, 653 F.3d at 6–7 (“The practical question inherent in the distinction between legislative and interpretive regulations is whether the new rule effects ‘a substantive regulatory change’ to the statutory or regulatory regime. . . . [T]he TSA’s policy *substantially changes the experience* of airline passengers and is therefore not merely ‘interpretative’ either of the statute directing the TSA to detect weapons likely to be used by terrorists or of the general regulation requiring that passengers comply with all TSA screening procedures.” (internal citations omitted) (emphasis added)).

¹¹³ *Id.* at 6–8.

of standing.¹¹⁴ RFRA specifically mandates that general Article III standing rules govern disputes under RFRA.¹¹⁵ The plaintiffs only asserted that one named party held religious objections to body scanners, but that party did not have proper standing.¹¹⁶ Therefore, the court dismissed the claim.¹¹⁷ Because no party with valid standing was before the court, this was the correct outcome.

F. FOURTH AMENDMENT CLAIM

The plaintiffs' claim with potentially the most import¹¹⁸ was that body scanner technology violates the Fourth Amendment.¹¹⁹ The D.C. Circuit held that body scanner screening does not violate the Fourth Amendment because of "the measures taken by the TSA to safeguard personal privacy" and because the Supreme Court has not held that the reasonableness of a search under the Fourth Amendment must be measured as "the least intrusive search practicable."¹²⁰

The D.C. Circuit began by noting that airport security searches are often analyzed using the administrative-search doc-

¹¹⁴ *Id.*

¹¹⁵ 42 U.S.C. § 2000bb-1 (2006) ("A person whose religious exercise has been burdened in violation of this section may assert that violation as a claim or defense in a judicial proceeding and obtain appropriate relief against a government. Standing to assert a claim or defense under this section shall be governed by the general rules of standing under article III of the Constitution.").

¹¹⁶ *Elec. Privacy Info. Ctr.*, 653 F.3d at 9.

¹¹⁷ *Id.* at 11. Note that even if a party with proper standing were to raise a religious issue with body scanners, it would be unlikely to succeed. The government cannot regulate an individual's approach, practice, or belief in religion. *See* U.S. CONST. AMEND. I; *Elk Grove Unified Sch. Dist. v. Newdow*, 542 U.S. 1, 48–49 (2004) (Thomas, J., concurring) ("[T]he Establishment Clause 'prohibits government from appearing to take a position on questions of religious belief.'" (citing *Cnty. of Allegheny v. ACLU*, 492 U.S. 573, 594 (1989))). But where a compelling government interest—for example, preventing mass terrorist attacks on the nation's air travel industry—exists, it can outweigh the individual's interest in free practice of religion. *See* Religious Freedom Restoration Act, 42 U.S.C. § 2000bb-1; *Wisconsin v. Yoder*, 406 U.S. 205, 215 (1972); *Sherbert v. Verner*, 374 U.S. 398, 404 (1963).

¹¹⁸ The Fourth Amendment protects an individual's "sacred" right to privacy. *See, e.g., Katz v. United States*, 389 U.S. 347, 351 (1967) ("[T]he Fourth Amendment protects people."); *see also* *Fixel v. Wainwright*, 492 F.2d 480, 483 (5th Cir. 1974) ("The sacredness of a person's . . . right of personal privacy and individuality are paramount considerations in our country and are specifically protected by the Fourth Amendment.").

¹¹⁹ *Elec. Privacy Info. Ctr.*, 653 F.3d at 10.

¹²⁰ *Id.*

trine, which it also claimed to use in this case.¹²¹ The administrative-search analysis includes three factors, as established by the Supreme Court in *Brown v. Texas*.¹²² But the D.C. Circuit analyzed only two of the factors, ignoring the third to reach its chosen outcome.¹²³

To support its two-factor administrative-search analysis, the D.C. Circuit relied on inapplicable cases. Rather than use the rule from *United States v. Hartwell*¹²⁴—an airport search case applying the administrative-search exception—the D.C. Circuit instead cited *United States v. Knights*¹²⁵ for the proposition that the administrative-search balancing test weighs only the search's intrusion on privacy against "the degree to which it is needed for the promotion of legitimate government interests."¹²⁶ While it may raise an eyebrow that *Knights* is not an airport security case,¹²⁷ further cause for concern arises because *Knights* is not even an administrative-search case. In *Knights*, the Supreme Court considered the constitutionality of a probationary search supported by reasonable suspicion.¹²⁸ But reasonable suspicion does not exist in the administrative-search context—particularly not for administrative searches in the airport security context. If reasonable suspicion were present, the Fourth Amendment would not mandate a showing of government interest to justify a search. The reasonable suspicion itself would make the search reasonable. But in the administrative-search context—*e.g.*, at airport security checkpoints—there is no reasonable suspicion, so the reasonableness test must take into account other factors—specifically, those laid down in *Brown*.¹²⁹

The plaintiffs argued that "using AIT for primary screening violates the Fourth Amendment because it is more invasive than

¹²¹ *Id.*

¹²² 443 U.S. 47, 51 (1979).

¹²³ *Elec. Privacy Info. Ctr.*, 653 F.3d at 10. Some have argued that because courts do not correctly apply the administrative-search exception in airport security cases, a different analytical framework ought to apply. *E.g.*, R. Gregory Israelsen, *Applying the Fourth Amendment's National-Security Exception to Airport Security and the TSA*, 78 J. AIR L. & COM. (forthcoming 2013) (arguing that courts should apply the national-security exception when considering airport security cases).

¹²⁴ *United States v. Hartwell*, 436 F.3d 174, 178 (3d Cir. 2006); *see infra* Part II.B.

¹²⁵ 534 U.S. 112 (2001).

¹²⁶ *Elec. Privacy Info. Ctr.*, 653 F.3d at 10.

¹²⁷ There are many airport security cases that the court could have referenced for the rule. *E.g.*, *Hartwell*, 436 F.3d at 178–79.

¹²⁸ *Knights*, 534 U.S. at 114.

¹²⁹ *See Brown v. Texas*, 443 U.S. 47, 50–51 (1979).

necessary to detect weapons or explosives.”¹³⁰ In other words, the plaintiffs claimed that body scanners are too invasive for use as a primary screening method; if used, scanners ought to only perform secondary screening as part of an escalating series of searches. One case that the plaintiffs relied on for this argument was *United States v. Hartwell*.¹³¹

In *Hartwell*, the Third Circuit relied on the rule from *Brown v. Texas*.¹³² “Suspicionless searches are permissible under the Fourth Amendment when a court finds a favorable balance between ‘the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty.’”¹³³ The court in *Hartwell* then analyzed an airport checkpoint search—notably pre-AIT—under the three-prong *Brown* test: (1) the importance of “preventing terrorist attacks on airplanes”; (2) whether airport checkpoints “advance the public interest”; and (3) whether “the procedures involved in Hartwell’s search were minimally intrusive.”¹³⁴ Examining the D.C. Circuit’s analysis in light of *Brown* reveals that the court failed to adequately address the second factor and completely ignored the third.

The D.C. Circuit failed to adequately address the second *Brown* factor because it did not analyze the effectiveness of AIT scanners in improving airport security. As the Supreme Court said in *City of Indianapolis v. Edmond*, a court “must look more closely at the nature of the public interests.”¹³⁵ This not only applies to the first *Brown* factor—the public’s interest in air safety—but also reasonably applies to the second *Brown* factor—whether the procedure in question *advances* the public interest.¹³⁶

In *EPIC*, the D.C. Circuit did not analyze the effectiveness of AIT scanners in improving airport security. The court simply concluded that “an AIT scanner, unlike a magnetometer, is capable of detecting, and therefore of deterring, attempts to carry

¹³⁰ *Elec. Privacy Info. Ctr.*, 653 F.3d at 10.

¹³¹ 436 F.3d 174.

¹³² *Brown*, 443 U.S. at 51.

¹³³ *Hartwell*, 436 F.3d at 178–79 (quoting *Illinois v. Lidster*, 540 U.S. 419, 427 (2004) (applying the rule from *Brown* in the highway checkpoint context)).

¹³⁴ *Id.* at 179–180.

¹³⁵ *City of Indianapolis v. Edmond*, 531 U.S. 32, 43 (2000).

¹³⁶ *Brown*, 443 U.S. at 51.

aboard airplanes explosives in liquid or powder form.”¹³⁷ But the court did not cite or reference any studies, expert opinions, or objective facts that could support such a conclusion.¹³⁸ The *Hartwell* court used a form of the word “effective” in four of its five sentences discussing the second *Brown* factor.¹³⁹ By contrast, the D.C. Circuit in *EPIC* did not deign to consider the *effectiveness*—which may be different than the capability—of body scanners to “detect[], and therefore . . . deter[], attempts to carry aboard airplanes explosives in liquid or powder form.”¹⁴⁰

The D.C. Circuit completely ignored the third *Brown* factor. In distinguishing *Hartwell*'s escalating-search approach, the court implicitly held that the third *Brown* factor did not apply, despite the Supreme Court's explicit guidance that all three factors apply in administrative-search cases.¹⁴¹

Because the D.C. Circuit misconstrued *Hartwell*'s footnote ten, it avoided applying the third *Brown* factor.¹⁴² The D.C. Circuit construed footnote ten to mean that “[n]othing in *Hartwell* . . . suggests the AIT scanners must be minimally intrusive to be consistent with the Fourth Amendment.”¹⁴³

But such a reading cannot logically follow from footnote ten. The *Hartwell* court noted, when beginning its analysis of the third *Brown* factor, what it was *not* doing: “set[ting] the outer limits of intrusiveness in the airport context.”¹⁴⁴ That is, while *Hartwell*'s search was minimally intrusive *in one way*, this does not mean that other procedures might not also be minimally intrusive (and therefore sufficiently unintrusive to meet the *Brown* standard of “the severity of the interference with individual liberty”).¹⁴⁵ This reading becomes even more inevitable in view of

¹³⁷ *Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 653 F.3d 1, 10 (D.C. Cir. 2011).

¹³⁸ This is significant because several researchers and security experts have questioned the effectiveness of body scanners at discovering explosives. *E.g.*, *Body Scanner Wouldn't Have Foiled Syringe Bomber, Says MP Who Worked on New Machines*, DAILY MAIL ONLINE (Jan. 3, 2010), <http://www.dailymail.co.uk/news/article-1240193/Body-scanner-wouldnt-foiled-syringe-bomber-says-MP-worked-new-machines.html>.

¹³⁹ *Hartwell*, 436 F.3d at 179–80.

¹⁴⁰ *Elec. Privacy Info. Ctr.*, 653 F.3d at 10.

¹⁴¹ *See, e.g.*, *Illinois v. Lidster*, 540 U.S. 420, 427 (2004) (quoting *Brown*, 443 U.S. at 51). Ironically, the D.C. Circuit cited *Illinois v. Lidster* earlier in its Fourth Amendment analysis. *Elec. Privacy Info. Ctr.*, 653 F.3d at 10.

¹⁴² *Elec. Privacy Info. Ctr.*, 653 F.3d at 11; *Hartwell*, 436 F.3d at 180 n.10.

¹⁴³ *Elec. Privacy Info. Ctr.*, 653 F.3d at 11.

¹⁴⁴ *Hartwell*, 436 F.3d at 180 n.10.

¹⁴⁵ *Brown*, 443 U.S. at 41.

the footnote's second sentence, in which the *Hartwell* court declined to "devise any bright-line test to implement the *Brown* standard in all future cases."¹⁴⁶

United States v. Aukai went even further than *Hartwell* in holding that a search must be minimally intrusive.¹⁴⁷ There, the Ninth Circuit considered whether the Fourth Amendment allowed a series of increasingly intrusive search techniques at an airport security checkpoint.¹⁴⁸ The court said that "[a] particular airport security screening search is constitutionally reasonable provided that it 'is no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives and that it is confined in good faith to that purpose.'"¹⁴⁹ Despite the plain language of the precedent it cited,¹⁵⁰ the D.C. Circuit held that there is effectively no limit on the scope of airport searches.¹⁵¹

In *Hartwell*, the Third Circuit spent a significant amount of time considering the third *Brown* factor—the level of intrusiveness of the search procedure under review.¹⁵² Because the D.C. Circuit misconstrued *Hartwell*'s footnote ten commentary, the court did not actually consider *how* AIT was "minimally intrusive."¹⁵³ The D.C. Circuit simply moved on after expressly rejecting the idea that a search ought to be minimally intrusive to protect privacy.¹⁵⁴ An escalating-search procedure—such as the one approved of in *Hartwell*—could work well in the AIT scanner context. A passenger who sets off an alarm—whether by magnetometer, wand, X-ray scan of carry-on baggage, or behavioral analysis—could be pulled aside for additional screening, which might include an AIT scan or enhanced pat-down. Such an escalating-search procedure could, as *Hartwell* pointed out, "make airport screening procedures minimally intrusive."¹⁵⁵

¹⁴⁶ *Hartwell*, 436 F.3d at 180 n.10.

¹⁴⁷ *United States v. Aukai*, 497 F.3d 955 (9th Cir. 2007).

¹⁴⁸ *Id.*

¹⁴⁹ *Id.* at 962 (quoting *United States v. Davis*, 482 F.2d 893, 913 (9th Cir. 1973)).

¹⁵⁰ Among other cases, *Hartwell* and *Aukai*.

¹⁵¹ *Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 653 F.3d 1, 11 (D.C. Cir. 2011) ("Nothing in *Hartwell* . . . suggests the AIT scanners must be minimally intrusive to be consistent with the Fourth Amendment.").

¹⁵² See *United States v. Hartwell*, 436 F.3d 174, 180 (3d Cir. 2006).

¹⁵³ *Elec. Privacy Info. Ctr.*, 653 F.3d at 10.

¹⁵⁴ *Id.* ("Nothing in *Hartwell* . . . suggests the AIT scanners must be minimally intrusive to be consistent with the Fourth Amendment.").

¹⁵⁵ *Hartwell*, 436 F.3d at 180.

In examining the third *Brown* factor, the Third Circuit in *Hartwell* looked at other factors besides the escalating nature of the search. *Hartwell* considered the stigma of being searched, the potential for abuse, the airlines' interests in protecting passengers, and the reduction in offensiveness due to notice.¹⁵⁶ The D.C. Circuit considered none of these factors, which may also affect the outcome of a *Brown* analysis. For example, the public's visceral reaction to body scanners and enhanced pat-downs may indicate that there is a significantly greater stigma attached to such a search than to a traditional magnetometer.¹⁵⁷

AIT also represents an enhanced potential for abuse. Despite the TSA's claim that it "distort[s] the image created using AIT and delet[es] it as soon as the passenger has been cleared,"¹⁵⁸ there have been multiple reported instances of TSA officers not following deletion protocol and scanners not being properly configured.¹⁵⁹ The Supreme Court does not trust the government to keep its promises to use overbroad grants of power only within certain bounds.¹⁶⁰ The TSA's failure to adhere to its own promised privacy protocols ought to have informed the D.C. Circuit's decision in its analysis of passenger privacy and AIT technology.

Regarding the failure to provide notice, the entire point of the *EPIC* lawsuit was that the TSA did not hold a notice-and-comment period before instituting AIT scanners as the primary screening method nationwide. While the court acknowledged that the TSA was wrong in failing to do so,¹⁶¹ it did not analogize *Hartwell* to make the connection that such a failure to provide notice may increase the offensiveness—and therefore intrusiveness—of a search.

¹⁵⁶ *Id.*

¹⁵⁷ See *supra* Part I.

¹⁵⁸ *Elec. Privacy Info. Ctr.*, 653 F.3d at 10.

¹⁵⁹ Johnson, *supra* note 3. But cf. Bob Burns, *TSA Response to "Feds Admit Storing Checkpoint Body Scan Images"*, TSA BLOG (Aug. 6, 2010), <http://blog.tsa.gov/2010/08/tsa-response-to-feds-admit-storing.html> (pointing out that the U.S. Marshals incident was at a Florida courthouse checkpoint, not an airport, and asserting that airport scanners do not store images).

¹⁶⁰ *United States v. Stevens*, 559 U.S. 460, 480 (2010) ("We would not uphold an unconstitutional statute merely because the [g]overnment promised to use it responsibly.").

¹⁶¹ *Elec. Privacy Info. Ctr.*, 653 F.3d at 11.

The only privacy considerations that the court offered—presumably coming from the TSA¹⁶²—were red herrings¹⁶³: “[D]istorting the image created using AIT and deleting it as soon as the passenger has been cleared.”¹⁶⁴ Pointing out what the TSA is *not* doing (i.e., how much worse the privacy intrusion could be) does not address the real question, which is what the TSA *is* doing (i.e., how much the search actually intrudes on privacy).¹⁶⁵ The fact that a government employee deletes an image that some perceive to be similar to an image of an unclothed passenger¹⁶⁶ is likely of little comfort to a passenger leaving a security checkpoint when she considers whether her privacy has been violated.¹⁶⁷

Another logical failure committed by the D.C. Circuit in support of its privacy argument was that the passenger could decide

¹⁶² Presumably, the court used the privacy considerations raised by the TSA in its briefs.

¹⁶³ See Cory S. Clements, Comment, *Perception and Persuasion in Legal Argumentation: Using Informal Fallacies and Cognitive Biases to Win the War of Words*, 2013 BYU L. REV. 319, 349 n.162 (noting that the red herring fallacy “comes from the sport of fox hunting in which a dried, smoked herring, which is red in color, is dragged across the trail of the fox to throw the hounds off the scent,” and that a “‘red herring’ argument . . . distracts the audience from the issue in question through the introduction of some irrelevancy”).

¹⁶⁴ *Elec. Privacy Info. Ctr.*, 653 F.3d at 10.

¹⁶⁵ That is, the TSA is saying that it could not distort the images and it could not delete them, and therefore it is protecting privacy by saying that it is not doing so. But if a person on trial for battery argues that stabbing her victim did not constitute battery because she did not shoot the victim, that means nothing with respect to whether she committed battery. Similarly, arguing that AIT scanners distort and do not save images means nothing for the argument as to whether they actually violate privacy.

¹⁶⁶ One rather provocative, well-known image of a woman allegedly created by inverting a body scan went viral in early 2010. See Adam Frucci, *Is It This Easy to Pull Straight Nude Pics from Airport Scanners? [NSFW]*, GIZMODO (Jan. 8, 2010), [http://gizmodo.com/5443901/is-it-this-easy-to-pull-straight-nude-pics-from-airport-scanners-\[nsfw\]](http://gizmodo.com/5443901/is-it-this-easy-to-pull-straight-nude-pics-from-airport-scanners-[nsfw]). The images turned out to be fake, but the public’s widespread reaction indicates that it perceives the TSA’s body scanners as presenting privacy concerns. See also Kashmir Hill, *These TSA Porn Photos Would Be Alarming—If They Were Real*, TRUE/SLANT (Jan. 27, 2010), <http://trueslant.com/KashmirHill/2010/01/27/tsa-scanner-porn-hoax-fools-gizmodo-drudge-report/>.

¹⁶⁷ One writer expressed dismay about officer conduct and body scanners after learning that some TSA officers were allegedly “laughing and clowning in regard to some . . . nude images.” Emma Barker, *The TSA Is Laughing at You*, COSMOPOLITAN (Dec. 28, 2012), <http://www.cosmopolitan.com/celebrity/news/tsa-laugh-at-bodies>. But cf. Bob Burns, *Body Scanner Resolution Rooms Conduct & Privacy*, TSA BLOG (Jan. 2, 2013), <http://blog.tsa.gov/2013/01/body-scanner-resolution-rooms-conduct.html> (disputing that officers gather in body scanner image-viewing rooms).

how to be violated: “any passenger may opt-out of AIT screening in favor of a [pat-down], which allows him to decide which of the two options for detecting a concealed, [non-metallic] weapon or explosive is least invasive.”¹⁶⁸ But such a Morton’s fork¹⁶⁹ is not what the Fourth Amendment intended; for example, initial screenings in *Hartwell* involved “less intrusive substitute[s] for a physical pat-down” and “no physical touching.”¹⁷⁰ The logical conclusion from reading *Hartwell* is that a physical pat-down is even more intrusive—and therefore less likely to meet the third *Brown* factor—than another search procedure. Therefore, an enhanced pat-down—cited approvingly by the D.C. Circuit—is likely cold comfort to those passengers who wish to avoid the privacy intrusion of an AIT scan.

The D.C. Circuit’s Fourth Amendment analysis of body scanners should not be relied upon by future courts. The court relied on overly attenuated case law to extract the wrong rule for administrative searches. It then failed to sufficiently analyze the second *Brown* factor and incorrectly ignored the third *Brown* factor. Because the D.C. Circuit’s analysis was so flawed, it should not be relied on by future courts. This failure to correctly apply case law or logic is an especially grievous sin because *EPIC* is currently the only appellate case to analyze the constitutionality of body scanners.

G. THE COURT’S FLAWED CONCLUSION

Regardless of the merits of the statutory or constitutional claims, the court’s outcome in light of the notice-and-comment findings was flawed. The court ordered the TSA to engage in notice-and-comment proceedings.¹⁷¹ After doing so, the D.C. Circuit cited “the obvious need for the TSA to continue its air-

¹⁶⁸ *Elec. Privacy Info. Ctr.*, 653 F.3d at 10.

¹⁶⁹ Scott Moise, *The Scrivener*, 22 S.C. LAW. 44, 45 (2011).

A Morton’s Fork is a practical dilemma in which two choices or alternatives are disadvantageous to or discredit the user. The term is named for John Morton, the Archbishop of Canterbury and Henry VII’s minister, who used a method of taxing that collected from everyone based on the following reasoning: the rich could afford to pay, and the poor must have accumulated savings from living frugally.

Id.

¹⁷⁰ *United States v. Hartwell*, 436 F.3d 174, 180 (3d Cir. 2006).

¹⁷¹ *Elec. Privacy Info. Ctr.*, 653 F.3d at 11.

port security operations without interruption” and did not force the TSA to suspend the rule in the meantime.¹⁷²

But the court never explained why there was an “obvious need” for the TSA to continue to use body scanners as an airport security measure.¹⁷³ Of course airports need security measures, but it does not necessarily follow that those security measures must include body scanners. This seems particularly obvious in light of the fact that at the time of the opinion, not even a year had passed since the TSA began to use body scanners as the primary screening method nationwide.¹⁷⁴

And if there were an “obvious need” to use body scanners, then the plaintiffs would not have brought suit. But because questions surrounding body scanners—particularly their efficacy and safety—remained unanswered, the plaintiffs brought suit to force a formal public rulemaking process.¹⁷⁵ Such a process could help the agency and the public understand the issues surrounding body scanners through a transparent discussion.

The court’s claim that the TSA cannot stop using body scanners—even temporarily—is further marred by the simple fact that the court ordered notice-and-comment proceedings.¹⁷⁶ There are three possible outcomes of notice-and-comment proceedings: no change to the rule, an amendment of the rule, or a repeal of the rule.¹⁷⁷ Therefore, implicit in the court’s order for the TSA to conduct notice-and-comment proceedings is an acknowledgment that something about the use of body scanners may need to change. For if there were no *possibility* for change, there would be no point to a notice-and-comment proceeding. Thus, by ordering a notice-and-comment proceeding, the court implicitly acknowledged that the rule might change.

But the acknowledgment that something about the rule might change contradicts the court’s implicitly claimed “looming specter of inutterable horror”¹⁷⁸ that would result from the interruption of the use of body scanners. Because notice-and-comment proceedings may result in a disruption of the use of body scan-

¹⁷² *Id.*

¹⁷³ *Id.*

¹⁷⁴ *Id.* at 3. In fact, body scanners had not been used for almost the entire decade following 9/11. *See id.*

¹⁷⁵ *Id.*

¹⁷⁶ *Id.* at 11.

¹⁷⁷ Administrative Procedure Act, 5 U.S.C. § 553(c) (2012).

¹⁷⁸ *Arizona v. United States*, 132 S. Ct. 2492, 2521 (2012) (Scalia, J., dissenting).

ners, it does not make sense for the court to order the TSA to hold a notice-and-comment proceeding on the use of body scanners and in the same breath claim that the TSA cannot be interrupted in its use of body scanners—precisely because a notice-and-comment proceeding may result in such a disruption.

V. CONCLUSION

The D.C. Circuit's ruling in *EPIC* was so flawed that no court should rely on it as precedent—especially as an issue of first impression. The court's logical errors were legion. Furthermore, the court relied on overly attenuated case law to arrive at its desired outcome.

The public and future courts have the right to well-reasoned, logically sound, and precedentially consistent opinions. When courts fail to produce such opinions, it leaves the public and future courts in the dark about what the law is and how it applies. Particularly because many of the substantive issues surrounding body scanners—including questions about their constitutionality—have never been considered by any other appellate court, the D.C. Circuit's epic failure in *EPIC* is particularly troubling.

As a concluding note, all hope for appellate guidance on body scanners is not lost. The TSA in early 2013 announced that it would no longer use backscatter-imaging scanners, opting instead to use only the more privacy-protective millimeter-wave scanners.¹⁷⁹ A few months later, in April 2013, nearly three years after the D.C. Circuit issued its opinion with the mandate “to act promptly on remand to cure the defect” (a lack of notice-and-comment proceedings) in the rule's promulgation,¹⁸⁰—and nearly two years after a follow-up order—the TSA initiated notice-and-comment proceedings on body scanners.¹⁸¹ The public finally had the chance to weigh in on the TSA's use of body scanners.¹⁸² The agency's final rule is due to issue in June

¹⁷⁹ See Nixon, *supra* note 58, and accompanying text.

¹⁸⁰ *Elec. Privacy Info. Ctr.*, 653 F.3d at 8.

¹⁸¹ Passenger Screening Using Advanced Imaging Technology, 78 Fed. Reg. 18,287 (proposed Mar. 26, 2013).

¹⁸² Susan Stellin, *Trying Passenger Patience*, N.Y. TIMES (Apr. 15, 2013), <http://www.nytimes.com/2013/04/16/business/public-pours-scorn-on-airport-body-scanners.html>.

2014.¹⁸³ That rule may be subject to judicial review, giving the D.C. Circuit the opportunity to clarify or correct its logical and reasoning errors in *EPIC* regarding the substantive statutory and constitutional questions surrounding the use of body scanners at airport security checkpoints.

¹⁸³ *Passenger Screening Using Advanced Imaging Technology*, FED. REG., <http://www.federalregister.gov/regulations/1652-AA67/passenger-screening-using-advanced-imaging-technology> (last visited Nov. 24, 2013).