Boston College Law Review

Volume 53
Issue 6 *Electronic Supplement*

Article 15

4-20-2012

Violating Privacy in Private: How *Epic v. DHS* Creates an Impossible Burden on Plaintiffs Trying to Demonstrate a Privacy Act Violation

David Gusella
Boston College Law School, david.gusella@bc.edu

VIOLATING PRIVACY IN PRIVATE: HOW *EPIC v. DHS* CREATES AN IMPOSSIBLE BURDEN ON PLAINTIFFS TRYING TO DEMONSTRATE A PRIVACY ACT VIOLATION

Abstract: On July 15, 2011, in *Electronic Privacy Information Center v. U.S. Department of Homeland Security,* the U.S. Court of Appeals for the D.C. Circuit held that to prove a violation of the Privacy Act, a plaintiff must show evidence of specific conduct. Yet, the current system of Freedom of Information Act exceptions and presumptions makes it exceedingly difficult for a plaintiff to gain access to evidence of specific conduct. Therefore, this Comment argues that these presumptions make it almost impossible for a plaintiff to discover and sue a defense agency for a Privacy Act violation, thereby leaving no realistic opportunity for relief to aggrieved parties.

Introduction

In 2007, the Transportation Security Administration (TSA) began using Advanced Imaging Technology (AIT) in body scanners at airport security checkpoints across the United States.[1] When a person stands in a scanner using AIT, the machine generates an image of the individual's naked body.[2] That image is then used to ensure that the traveler is not trying to carry weapons or explosives onto an airplane.[3] Due to the private nature of one's naked body, many individuals have attempted to sue the government to prevent these scanners from being used.[4] They have done so by claiming that use of AIT scanners constitutes an unconstitutional search which unreasonably intrudes on individuals' privacy.[5]

On July 15, 2011, in *Electronic Privacy Information Center v. U.S. Department of Homeland Security* (*EPIC II*), the U.S. Court of Appeals for

---

[1] Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec. (*EPIC II*), 653 F.3d 1, 3 (D.C. Cir. 2011) (en banc).

[2] *Id.* (citing 49 U.S.C. §§ 44901(a), 44902(a)(1) (2007)).

[3] *Id.* (citing §§ 44901(a), 44902(a)(1)).

[4] *See id.*; Roberts v. Napolitano, 798 F. Supp. 2d 7, 9–12 (D.D.C. 2011); Redfern v. Napolitano, No. 10-12048-DJC, 2011 WL 1750445, at *3–8 (D. Mass. May 9, 2011).

[5] *See EPIC II,* 653 F.3d at 3; *Roberts,* 798 F. Supp. 2d at 9–12; *Redfern,* 2011 WL 1750445, at *3–8.

the D.C. Circuit held that the TSA did not follow proper administrative procedures in employing these scanners.[6] Nonetheless, the court held that the TSA's use of AIT scanners did not violate the Privacy Act or constitute an unreasonable search in violation of the Fourth Amendment.[7]

Part I of this Comment outlines the use of AIT and the Electronic Privacy Information Center's (EPIC) suit against the TSA.[8] Then, Part II explains the court's reasoning in concluding that the use of AIT does not violate the Privacy Act.[9] Finally, Part III argues that the presumptions for the government and the exceptions built into the Freedom of Information Act (FOIA) prevent plaintiffs from obtaining sufficient evidence to sue defense agencies for Privacy Act violations.[10] It further contends that these presumptions are so strong that it is almost impossible for a plaintiff to engage in discovery and successfully sue a defense agency for a Privacy Act violation.[11]

I. Background of *EPIC v. DHS*

A. *The Development and Use of AIT*

After September 11, 2001, when terrorists used box cutters and small knives to hijack commercial planes and fly them into the World Trade Center Towers in New York City and the Pentagon in Washington, D.C., Congress passed expansive airline security legislation.[12] This legislation made all airport screeners federal TSA employees within the Department of Homeland Security (DHS).[13] Furthermore, Congress required all commercial airline passengers to be screened by TSA agents to ensure that those passengers are not carrying weapons or explosives.[14] In addition, Congress authorized the TSA to determine confidential standard operating procedures for the screening process.[15] Congress also barred anyone who had not been screened by TSA

---

[6] 653 F.3d at 7–8.

[7] *See id.* at 10–11.

[8] *See infra* notes 12–54 and accompanying text.

[9] *See infra* notes 55–74 and accompanying text.

[10] *See infra* notes 75–91 and accompanying text.

[11] *See infra* notes 85–91 and accompanying text.

[12] *See* Aviation and Transportation of Security Act, Pub. L. No. 107-71, 115 Stat. 597 (codified in scattered sections of 49 U.S.C.); 5 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 10.6(a) (4th ed. 2010).

[13] Pub. L. No. 107-71, 115 Stat. 597 (codified in scattered sections of 49 U.S.C.).

[14] *EPIC II,* 653 F.3d at 3 (citing 49 U.S.C. §§ 44901(a), 44902(a)(1) (2007)).

[15] *Id.*

agents from entering the "sterile area" of an airport, the area one enters after passing through security.[16]

In the Intelligence Reform and Terrorism Prevention Act of 2004, Congress directed the TSA to prioritize the development of new technology that can test for nonmetallic, chemical, biological, and radiological weapons in all forms.[17] To achieve these ends, the TSA contracted with private vendors to develop AIT.[18] Vendors produced two different types of scanners: one that uses millimeter wave technology, which employs radio frequency energy, and one that uses backscatter technology, which employs low-intensity x-ray beams.[19] Both scanners generate an image of an unclothed person, allowing the operator of the machine to search for nonmetallic objects without having to pat down a passenger.[20]

Although many passengers complain about being forced to undergo AIT scans, the TSA contends that passengers are not required to submit to a scan.[21] Instead, passengers may opt for a pat down, which the TSA claims is the only effective alternative method of screening passengers.[22] Still, many passengers are unaware that the pat-down option exists.[23] In addition, some passengers who have opted for a pat down complain that the resulting pat down was unnecessarily aggressive.[24]

The TSA has taken steps to address concerns regarding passengers' privacy and safety.[25] For example, each image produced by the scanner passes through a filter to obscure facial features and is only viewable by an officer on a computer screen in a remote and secure room.[26] As soon as the passenger is cleared, the image is deleted.[27] The officer cannot save the image, and no recording devices are allowed in the secure room.[28] In addition, the TSA commissioned two studies that have concluded that the backscatter scanners emit levels of radiation

---

[16] *Id.* (citing 49 C.F.R. § 1540.105(a)(2) (2003)).
[17] 49 U.S.C. § 44925(a).
[18] *EPIC II,* 653 F.3d at 3.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *EPIC II,* 653 F.3d at 3.
[25] *Id.* at 4.
[26] *Id.*
[27] *Id.*
[28] *Id.*

well within acceptable limits, even for frequent travelers.[29] The millimeter wave scanners have also been tested to confirm that they meet accepted safety standards.[30]

B. *EPIC's Suit Against the Government*

In April and July of 2009, EPIC submitted two separate Freedom of Information Act (FOIA) requests to DHS seeking information regarding TSA's use of AIT.[31] In the first FOIA request, EPIC sought documents relating to the training and operation of these scanners and information about the scanners' capabilities to store images.[32] In its second request, EPIC sought uncensored images from these scanners, contracts relating to the use and manufacture of AIT, and complaints to the TSA about the use of AIT.[33]

In response to these requests, DHS produced 1766 pages of responsive documents, many of which were heavily redacted.[34] DHS also withheld 2000 images produced by the body scanners and 376 pages of TSA training materials.[35] According to the TSA, the withheld images portrayed various threat objects dispersed over the body and were meant to test the detection standards in the TSA's procurement specifications.[36] In addition, the TSA withheld the 376 pages of security training materials because they were created to train TSA employees who operate the body scanners.[37] The TSA claimed that the release of these images and documents would threaten transportation security.[38]

On November 5, 2009, EPIC sued DHS for failing to respond to its first FOIA request in a timely manner.[39] On January 13, 2010, EPIC again sued DHS for failing to respond to its second FOIA request in a timely manner.[40] The U.S. District Court for the District of Columbia consolidated these suits, and on January 12, 2011 it held that a FOIA

---

[29] *Id.*

[30] *EPIC II,* 653 F.3d at 4.

[31] Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec. (*EPIC I*), 760 F. Supp. 2d 4, 7–8 (D.D.C.), *motion for relief from judgment denied,* 653 F.3d 1 (D.C. Cir. 2011).

[32] *Id.* at 8 n.2.

[33] *Id.*

[34] *Id.*; *see FOIA Note #20 (Aug. 15, 2011): Government Transparency,* Elec. Privacy Info. Ctr. (Aug. 15, 2011), http://epic.org/foia_notes/foia_note_20_august_15_2011.html.

[35] *EPIC I,* 760 F. Supp. 2d at 8.

[36] *Id.*

[37] *Id.* at 8–9.

[38] *Id.*

[39] *Id.* at 9.

[40] *Id.*

exception permitted the TSA to withhold images and training materials from EPIC.[41]

In the meantime, more than thirty organizations, including EPIC, had sent a letter to the Secretary of Homeland Security objecting to the use of AIT scanners as a primary means of screening passengers.[42] They asked that the TSA cease using AIT in that capacity pending a ninety-day formal public rulemaking process.[43] The TSA responded with a letter, which addressed these organizations' concerns, but ignored their request for a formal rulemaking process.[44]

In April of 2010, EPIC and a slightly different group of organizations sent a petition to the Secretary and Chief Privacy Officer of DHS.[45] This petition was made under the Administrative Procedures Act, which allows "an interested person the right to petition for the issuance, amendment, or repeal of a rule."[46] In this petition, the group argued that the use of AIT for primary screening violates the Privacy Act, as well as a variety of other statutes and Constitutional rights.[47] In May of 2010, the TSA again responded by letter, clarifying some factual matters and defending its position that it is not required to initiate a rulemaking process each time it changes screening procedures.[48]

Other individuals and organizations, who were also concerned with the use of AIT, brought suit against the TSA.[49] Those suits were unsuccessful, however, and the U.S. District Courts for the Districts of Columbia and Massachusetts dismissed claims against the TSA, holding that under the U.S. Code, the only court with original jurisdiction for challenges to the use of AIT scanners is the D.C. Circuit.[50] Accordingly,

---

[41] *EPIC I,* 760 F. Supp. 2d at 9, 13, 14.

[42] *EPIC II,* 653 F.3d at 4; Letter from Am. Ass'n of Small Prop. Owners et al., to Janet Napolitano, Sec'y, Dep't of Homeland Sec. (May 31, 2009), *available at* http://epic.org/privacy/airtravel/backscatter/Napolitano_ltr-wbi-6–09.pdf.

[43] *EPIC II,* 653 F.3d at 4.

[44] *Id.*

[45] *Id.*; Letter from Elec. Privacy Info. Ctr. et al., to Janet Napolitano, Sec'y, Dep't of Homeland Sec., and Mary Ellen Callahan, Chief Privacy Officer, Dep't of Homeland Sec. (Apr. 21, 2010), *available at* http://epic.org/privacy/airtravel/backscatter/petition_042110.pdf.

[46] *EPIC II,* 653 F.3d at 4; *see* 5 U.S.C. § 553(e) (2006).

[47] *EPIC II,* 653 F.3d at 4.

[48] *Id.*

[49] *See Roberts,* 798 F. Supp. 2d at 9–12; *Redfern,* 2011 WL 1750445, at *3–8.

[50] *See Roberts,* 798 F. Supp. 2d at 9–12; *Redfern,* 2011 WL 1750445, at *3–8; *see also* 49 U.S.C.A. § 46110(a) (West 2003) (providing that a person with a substantial interest in an order by the Secretary of Transportation may apply for review of the order by filling a petition in the U.S. Court of Appeals for the D.C. Circuit or the circuit in which the person resides or has its principal place of business).

EPIC, joined by two members of its advisory board who had traveled frequently and been subjected to AIT screening by the TSA, petitioned the D.C. Circuit for review.[51]

On July 15, 2011, the court held that the TSA's adoption of AIT constituted a substantive legislative rule subjecting it to notice-and-comment rulemaking requirements.[52] Notice-and-comment rulemaking would require the TSA to publish the new rule, take comments on it from interested parties, and then respond to those comments before implementing the new rule.[53] In addition, the court held that AIT procedures did not violate the Privacy Act.[54]

II. Reasoning Behind the D.C. Circuit's Holding That the Use of AIT Does Not Violate the Privacy Act

A. *Record Keeping Practices Under the Privacy Act*

The *EPIC II* court held that a violation of the Privacy Act requires specific evidence of violation—in this case, evidence of images stored on AIT scanners, not just evidence of the scanners' capability to store images.[55] Furthermore, the court held that if the TSA linked names of passengers with images produced using AIT, this would constitute a "system of records" that would violate the requirements of the Privacy Act, which provides that such records not be kept unless public notice is given.[56] Yet because EPIC offered no evidence that the TSA in fact linked the names of passengers with body scan images, the court dismissed the Privacy Act claim.[57]

Nonetheless, EPIC did provide some evidence, contrary to TSA public statements that the memory software on all machines had been disabled, that thousands of images had been saved and that the machines had the capability to store and send images when in "test mode."[58] The court, however, deemed this evidence insufficient.[59] In

---

[51] *EPIC II,* 653 F.3d at 4.

[52] *Id.* at 6.

[53] *Id.* at 4–5.

[54] *Id.* at 8.

[55] Elec. Priv. Info. Ctr. v. U.S. Dep't of Homeland Sec. (*EPIC II*), 653 F.3d 1, 8 (D.C. Cir. 2011) (en banc).

[56] *See* 5 U.S.C. § 552a (West 2010); *EPIC II,* 653 F.3d at 8.

[57] *EPIC II,* 653 F.3d at 8.

[58] David B. Olson, *Naked Body Scans and Full-Body Pat-Downs: The Controversy Surrounding the TSA's Enhanced Airport Screening Procedures, in* 2011 Aspatore Special Report, Navigating the Legal Impact of Airport Security Measures: An In-Depth Look at Passenger Profiling and Its Effect on the Public 7 (2011).

supporting this conclusion it relied on the 1996 decision by the U.S. District Court for the District of Columbia, *Henke v. U.S. Department of Commerce.*[60] In *Henke,* the Department of Commerce's Advanced Technology Program (ATP) stored information about businesses to select and award grants for developing high-risk technologies.[61] The *Henke* court held that this information did not constitute a "system of records" requiring the government to disclose its recordkeeping practices under the Privacy Act.[62] Specifically, to prove a Privacy Act violation, the court required evidence that specific retrieval of personally identifiable information occurred, not just evidence that retrieval of this information from ATP databases was possible.[63] Yet in *Henke,* the court supported its conclusion that the records did not violate the Privacy Act by recognizing that the ATP gives grants to businesses and not individuals.[64]

B. *Exceptions to the FOIA*

The FOIA permits public access to any federal government record that is not specifically exempt from disclosure.[65] The FOIA contains exceptions allowing organizations to redact information for a variety of reasons.[66] For example, an agency can claim a FOIA exception if its

---

[59] *EPIC II,* 653 F.3d at 8.

[60] *See id.* (citing Henke v. U.S. Dep't of Commerce, 83 F.3d 1453, 1460–61 (D.C. Cir. 1996)).

[61] *Henke,* 83 F.3d at 1457.

[62] *Id.* at 1460–62.

[63] *Id.*

[64] *Id.* at 1461–62.

[65] 5 U.S.C. § 552 (West 2009); Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec. (*EPIC I*), 760 F. Supp. 2d 4, 10 (D.D.C. 2011).

[66] 5 U.S.C. § 552. Matters may be exempt if they are:

> (1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order; (2) related solely to the internal personnel rules and practices of an agency; (3) specifically exempted from disclosure by statute . . . (7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings . . . (7)(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law).

Id.

affidavits meet a three-part test.[67] In *EPIC I,* the TSA claimed that it could redact information under the (b)(2) exception, for matters related to the internal personnel rules and practices of the agency, and under the (b)(3) exception, which allows matters to be kept secret if exempted from disclosure by statute.[68] The court held in favor of the TSA on the (b)(2) exception and declined to rule on the validity of the (b)(3) exception.[69]

At the time of the decision, the (b)(2) exception fell into two main categories: "low (b)(2)" material, concerning relatively trivial internal agency matters, and "high (b)(2)" material, concerning internal agency information that, if disclosed, would risk enabling the requester of the information to circumvent the law.[70] In *EPIC I,* the court granted the TSA summary judgment, holding that the information could be withheld from EPIC under a "high (b)(2)" exception.[71]

Less than one year after the decision, however, in 2009, in *Milner v. Department of the Navy,* the U.S. Supreme Court held that the "high (b)(2)" exception does not exist and that exceptions to the FOIA should be read narrowly.[72] Further, the Court recognized that an amended version of another exception serves essentially the same purpose, shielding certain information compiled for law enforcement purposes if disclosure could reasonably be expected to risk circumvention of the law.[73] As a result, a court would likely allow the TSA to withhold or redact the same information from EPIC under that exception now that the Supreme Court has condemned the use of the "high (b)(2)" exception.[74]

---

[67] *See* Military Audit Project v. Casey, 656 F.2d 724, 738 (D.C. Cir. 1981). The three-part test states that summary judgment for an agency on the basis of its affidavits is appropriate if it:

> (a) Describes the documents and the justifications for nondisclosure with reasonably specific detail, (b) demonstrates that the information withheld logically falls within the claimed exemption, and (c) its statements are not controverted by either contrary evidence in the record nor by evidence of agency bad faith.

Id.

[68] *See* 5 U.S.C. § 552(b); *EPIC I,* 760 F. Supp. 2d at 13.

[69] *EPIC I,* 760 F. Supp. 2d at 13.

[70] Milner v. Dep't of Navy, 131 S. Ct. 1259, 1263 (2011).

[71] *EPIC I,* 760 F. Supp. 2d at 13, 14.

[72] *Milner,* 131 S. Ct. at 1263.

[73] *Id.*

[74] *See id.*; *EPIC I,* 760 F. Supp. 2d at 10–13.

III. Deference to the Executive Made It Impossible for EPIC to Meet Its Burden of Proving Specific Conduct

A. *Deference to the Executive*

In granting the TSA's motion for summary judgment, the court applied a rule that was highly deferential to the executive branch, allowing the government to meet its "high (b)(2)" burden easily while preventing EPIC from obtaining any evidence of specific conduct in violation of the Privacy Act.[75] In following this rule, the court held that it is well established that a court may rely on government affidavits to support the withholding of documents under FOIA exceptions and that the judiciary owes some measure of deference to the executive in cases implicating national security.[76]

Because of that deference, courts often decline to review documents in camera to determine whether FOIA exceptions apply, instead demanding only that the government "articulate a logical basis for classification."[77] Similarly, the *EPIC I* court concluded that it must grant summary judgment to the TSA if the government's affidavits met the three-part test of a FOIA exception.[78] The court held, however, that EPIC's evidence contrary to the TSA's public statements was not enough to destroy this presumption in favor of the TSA.[79] As a result, because the presumption in favor of the agency is so high and the information available to the plaintiff is so minimal, courts are not actually testing national security claims for reasonableness, good faith, specificity, and plausibility.[80]

Furthermore, the government can always argue that information should be withheld under a "mosaic theory."[81] Under that theory, almost all tiny pieces of information should be withheld or else they might be pieced together to produce an accurate picture of an entire

---

[75] *See* Elec. Priv. Info. Ctr. v. U.S. Dep't of Homeland Sec. (*EPIC II*), 653 F.3d 1, 8 (D.C. Cir. 2011) (en banc); Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec. (*EPIC I*), 760 F. Supp. 2d 4, 10–13 (D.D.C.), *motion for relief from judgment denied,* 653 F.3d 1 (D.C. Cir. 2011).

[76] *EPIC I,* 760 F. Supp. 2d at 12–13.

[77] Nathan F. Wessler, Note, *"[We] Can Neither Confirm Nor Deny the Existence or Nonexistence of Records Responsive to Your Request": Reforming the Glomar Response Under FOIA,* 85 N.Y.U. L. Rev. 1381, 1386 (2010).

[78] *EPIC I,* 760 F. Supp. 2d at 10; *see supra* note 67 and accompanying text.

[79] *See EPIC I,* 760 F. Supp. 2d at 10; Olson, *supra* note 58, at 7.

[80] *See EPIC I,* 760 F. Supp. 2d at 10; David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act,* 115 Yale L.J. 628, 637 (2005).

[81] *See* Pozen, *supra* note 80, at 643–44, 652.

agency's procedures or rules.[82] Thus, combined with a mosaic theory argument, the presumption in favor of the government could stretch, allowing an agency to withhold even the tiniest piece of useful information lest it be aggregated and used against the government.[83] Moreover, because a plaintiff like EPIC does not have access to any of this information, it can only insist that the agency's affidavit in support of summary judgment does not contain all the arguments required to meet a given exemption's requirements.[84]

B. *The Court of Appeals' Requirement of Specific Conduct Ignores EPIC's Previous Attempts to Obtain Information*

In addition, the *EPIC I* court required evidence of specific conduct to prove a Privacy Act violation, ignoring EPIC's previous failed attempts to obtain information through the FOIA.[85] In EPIC's original FOIA request in April of 2009, it sought numerous records including all documents concerning the capability of AIT to obscure, degrade, store, transmit, reproduce, retain, or delete images of individuals.[86]

The court in *EPIC I,* however, deferred to the judgment of the executive branch and allowed the TSA to use a high (b)(2) exception to the FOIA to redact and withhold many of the documents sought by EPIC, including sample images from the scanners, thereby making it impossible for EPIC to prove specific conduct.[87] Furthermore, the *EPIC II* court, by requiring evidence of specific conduct to demonstrate a national security agency's violation of the Privacy Act, ignored the unreasonably high burden necessary to meet that requirement.[88] On the one hand, an agency may not simply refuse to acknowledge that it maintains a system of records and thereby insulate itself from the reach of the Pri-

---

[82] *See id.*

[83] *See id.*

[84] *See* Justin Cox, *Maximizing Information's Freedom: The Nuts, Bolts, and Levers of FOIA,* 13 N.Y. City L. Rev. 387, 410–11 (2010).

[85] *See EPIC II,* 653 F.3d at 8; *EPIC I,* 760 F. Supp. 2d at 8, 10–13.

[86] *EPIC I,* 760 F. Supp. 2d at 8 n.2.

[87] *See id.* at 1013; *supra* notes 67–69 and accompanying text. The high (b)(2) exception allows information to be redacted that relates solely to the internal personnel rules and practices of an agency that, if disclosed, would risk enabling the requester of the information to circumvent the law. *See supra* notes 67–69 and accompanying text. Although the U.S. Supreme Court has since held that a high (b)(2) exception no longer exists, such matters can be redacted under exemption (7)(E), which protects information compiled for law enforcement purposes if disclosure could reasonably be expected to risk circumvention of the law. *See supra* notes 67–69 and accompanying text.

[88] *See EPIC II,* 653 F.3d at 8 (citing Henke v. U.S. Dep't of Commerce, 83 F.3d 1453, 1460–61 (D.C. Cir. 1996)); *EPIC I,* 760 F. Supp. 2d at 8.

vacy Act.[89] On the other hand, due to the exceptions to the FOIA and deference to the executive branch upheld by the court in *EPIC I,* the court in *EPIC II* relied on the TSA's affidavits to conclude that the TSA did not violate the Privacy Act.[90] As a result of the presumptions and exceptions within the Privacy Act and FOIA, defense agencies may violate the Privacy Act without any opportunity for legal recourse.[91]

Conclusion

EPIC's case against the TSA demonstrates the nearly impossible burden a plaintiff must meet to prove a security agency's specific conduct in violation of the Privacy Act. To prove specific conduct, a plaintiff needs to demonstrate specific instances of a government agency's storage of records in violation of the Privacy Act. A plaintiff's primary method to obtain this kind of classified information is through a FOIA request, but the exceptions to the FOIA and the presumptions in favor of the government in cases implicating national security prevent any plaintiff from obtaining this required information.

Thus, courts have created a presumption in favor of the government, even though the government is the only party with enough information to tailor its affidavits to the summary judgment standard. In addition, courts are hesitant to review these kinds of documents in camera. As a result, the only party with enough information to know about Privacy Act violations is the government. Therefore, the court has set a precedent allowing security agencies to potentially violate the Privacy Act with no realistic opportunity for relief available to aggrieved parties.

David Gusella

Preferred citation: David Gusella, Comment, *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 (2012), http://bclawreview.org/e-supp/2012/14_gusella.pdf.

---

[89] *Henke,* 83 F.3d at 1461.

[90] *See* Freedom of Information Act § 552(b), 5 U.S.C. § 552 (West 2009); *EPIC II,* 653 F.3d at 8; *EPIC I,* 760 F. Supp. 2d at 10–13; Pozen, *supra* note 80, at 643–44, 652.

[91] *See* 5 U.S.C. § 552; *EPIC II,* 653 F.3d at 8; *EPIC I,* 760 F. Supp. 2d at 10–13; Pozen, *supra* note 80, at 643–44, 652.