COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE U.S. CUSTOMS and BORDER PROTECTION of the
DEPARTMENT OF HOMELAND SECURITY

[DHS Docket Nos. 2012-0019 and 2012-0020]

Automated Targeting System
Notice of Privacy Act System of Records and
Proposed Rule: Privacy Act of 1974 Exemptions

June 21, 2012

TABLE OF CONTENTS

I. Introduction

By notices published on May 22, 2012[1] and May 23, 2012,[2] the United States Customs and Border Protection ("CBP") of the Department of Homeland Security ("DHS") seeks to exempt the Automated Targeting System ("ATS") from several significant provisions of the Privacy Act of 1974. Pursuant to the CBP notices, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy and security issues raised by the database, to urge that CBP cease retaining personal information on American citizens in the ATS, and to demand that CBP significantly narrow the Privacy Act exemptions for the system if the proposal goes forward. Additionally, EPIC notes that the proposed routine uses and exemptions are unlawful because they are "without observance of procedure required by law,"[3] and should therefore be withdrawn.

ATS was initially created to screen shipping cargo.[4] Over the last six years, CBP has expanded ATS to screen and monitor an ever-growing population of individuals, and create "risk assessment" profiles on Americans, suspected of no crime. While ATS may be an efficient tactic to screen cargo, it is unconstitutional, improper, and ineffective to screen individuals in the same manner. The ATS database contains an excess of personally identifiable information ("PII") ranging from names, addresses, nationalities, and Social Security Numbers to "information that could directly indicate the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, or sex life"

[1] Notice of Privacy Act System of Records, 77 Fed. Reg. 30297 (proposed May 22, 2012).
[2] Notice of Proposed Rulemaking, 77 Fed. Reg. 30433 (proposed May 23, 2012) (to be codified at 6 C.F.R. pt 5).
[3] The Administrative Procedure Act, 5 U.S.C. § 706 (2)(D) (2006). The proposed ATS changes are effective the same date on which the System of Records Notice ("SORN") comment period ends, and a day before the proposed exemption comment period ends. Therefore, the agency has no meaningful opportunity to consider comments as required by 5 U.S.C. § 553(c). Consequently, the proposed routine uses and exemptions are unlawful because they are "without observance of procedure required by law."
[4] Proposed Rule, 68 Fed. Reg. 43574 (proposed July 23, 2003) (codified at 19 C.F.R. pts. 4, 103, 113, 122, 123, 178, and 192).

of individuals.[5] On the basis of this information, and not any actual conduct, a federal agency of the United States makes determinations about the rights and opportunities of U.S. citizens.

Since 2006, EPIC has consistently recommended that CBP suspend ATS, or in the alternative, fully apply all Privacy Act safeguards to any person subject to ATS.[6] EPIC has also opposed other DHS passenger profiling programs,[7] and has called for an independent audit to determine whether the Transportation Security Administration ("TSA") airport screeners engage in racial profiling.[8] EPIC highlighted the problems inherent in passenger profiling systems such as ATS in previous testimony and comments. In testimony before the National Commission on Terrorist Attacks Upon the United States (more commonly known as "the 9/11 Commission"), EPIC President Marc Rotenberg explained, "there are specific problems with information technologies for monitoring, tracking, and profiling. The techniques are imprecise, they are subject to abuse, and they are invariably applied to purposes other than those originally intended."[9]

---

[5] 77 Fed. Reg. 30300.

[6] *See, e.g.*, EPIC et al., *Comments Urging the Department of Homeland Security To (A) Suspend the "Automated Targeting System" As Applied To Individuals, Or In the Alternative, (B) Fully Apply All Privacy Act Safeguards To Any Person Subject To the Automated Targeting System* (Dec. 4, 2006), *available at* http://epic.org/privacy/pdf/ats_comments.pdf; EPIC, *Comments on Automated Targeting System Notice of Privacy Act System of Records and Notice of Proposed Rulemaking, Docket Nos. DHS-2007-0042 AND DHS-2007-0043* (Sept. 5, 2007), *available at* http://epic.org/privacy/travel/ats/epic_090507.pdf. See also, EPIC: Automated Targeting System, https://epic.org/privacy/travel/ats/.

[7] *See, e.g.*, EPIC et al., *Comments on the Terrorist Screening Database System of Records, Notice of Privacy Act System of Records and Notice of Proposed rulemaking, Docket Nos. DHS 2011-0060 and DHS 2011-0061* (Aug. 5, 2011), *available at* http://epic.org/privacy/airtravel/Comments_on_DHS-2011-0060_and_0061FINAL.pdf; EPIC, *Comments on Secure Flight*, *Docket Nos. TSA-2007-28972, 2007-28572* (Sept. 24, 2007), *available at* http://epic.org/privacy/airtravel/sf_092407.pdf; EPIC, *Secure Flights Should Remain Grounded Until Security and Privacy Problems are Resolved, Spotlight on Surveillance Series* (August 2007), *available at* http://epic.org/privacy/surveillance/spotlight/0807/default.html; EPIC: Passenger Profiling, http://epic.org/privacy/airtravel/profiling.html; EPIC: Secure Flight, http://epic.org/privacy/airtravel/secureflight.html; EPIC: Air Travel Privacy, http://epic.org/privacy/airtravel/.

[8] Letter from EPIC et al., to Secretary Janet Napolitano and Honorable Charles K. Edwards, Department of Homeland Security (Dec. 1, 2011), *available at* http://epic.org/privacy/airtravel/12-01-11-Coalition-Racial-Profiling-Audit-DHS-Letter.pdf.

[9] Marc Rotenberg, President, EPIC, *Prepared Testimony and Statement for the Record of a Hearing on Security & Liberty: Protecting Privacy, Preventing Terrorism Before the National Commission on Terrorist Attacks Upon the United States* (Dec. 8, 2003), *available at* http://www.epic.org/privacy/terrorism/911commtest.pdf.

Despite EPIC's recommendations and empirical evidence of the ineffectiveness of passenger profiling, CBP continues to expand the ATS database and now proposes broad Privacy Act exemptions to the operation of the system.

II. ATS is a Massive Database that "Ingests" a Plethora of Personal Information from a Myriad of Sources

ATS collects, "ingests", and retains an exorbitant amount of PII from millions of people.[10] CBP uses ATS to monitor individuals and cargo that travel to, from, and throughout the United States. As described by CBP, ATS creates a "risk-based" assessment on individuals by "matching criteria comprising a targeting rule."[11] CBP then uses this "match and subsequent matches" to continually monitor the targeted individual.[12] Based upon the automated "risk assessment", individuals are subjected to further "scrutiny" and inspection, even if the individual has never been "previously associated with a law enforcement action or otherwise be[en] noted as a person of concern to law enforcement."[13] CBP alleges that individuals are not assigned risk scores, and that "risk assessment scores" are used solely for cargo or conveyances of interest."[14] CBP, however, admits that traveler risk assessments "compare[] PII . . . against lookouts and patterns of suspicious activity."[15] Therefore, no matter the terminology—"risk assessment match," "score," or "rule"—CBP uses PII to determine whether an individual, based on personal immutable, characteristics and not conduct, should undergo investigation, monitoring, and denial of her constitutional right to travel.[16] Moreover, because ATS risk assessment compares PII of individuals that have no criminal history against "patterns of suspicious activity," this increases the likelihood that

[10] The Research and Innovative Technology Administration's Bureau of Transportation Statistics reports that from March 2011 until February 2012, 642 million revenue passengers flew aboard U.S. aircraft. This number comprises only a fraction of the millions of individuals that are monitored with ATS. *See* Research and Innovative Technology Administration Bureau of Transportation Statistics, TranStats, http://www.transtats.bts.gov/(last visited June 6, 2012).
[11] Dep't of Homeland Sec., U.S. Customs and Border Protection, Privacy Impact Assessment for the Automated Targeting System, DHS/CBP/PIA-006(b), 19 (June 1, 2012) [hereinafter "ATS Privacy Impact Assessment"] *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_ats006b.pdf.
[12] *Id.*
[13] *Id*.
[14] *Id*.
[15] *Id*.
[16] *Sáenz v. Roe*, 526 U.S. 489 (1999).

CBP and ATS profile innocent individuals of certain racial, ethnic, or religious groups. For example, if past terrorist incidents have involved members of a certain ethnic group, then ATS may flag all members of that ethnic group with a higher "risk assessment" for terrorist behavior.

According to CBP, ATS is comprised of five modules that the agency says are designed to support CBP officers "in determining whether or not a particular individual or cargo is higher risk than other individuals or cargo."[17] The three modules of interests are ATS-Land ("ATS-L"), ATS-Passenger ("ATS-P"), and ATS-Targeting Framework ("ATS-TF").

ATS-TF is the most expansive module, permitting ATS users to search across all of the ATS modules and initiate investigations, exchange and disclose information, track, and save individual information across various databases.[18] These databases include DHS's Watchlist Service, the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System, and commercial data aggregators.[19] Alarmingly, this module even permits ATS users to include information gathered from public facing webpages into their reports.[20] False accusations over the internet that are provided by malicious actors could potentially be included into ATS reports. CBP could then use this misinformation to place individuals on terrorist watchlists.

The ATS-L module is used to analyze and create "risk assessments" of private passenger vehicles crossing U.S. borders.[21] CBP has previously touted ATS-L as "provid[ing], within seconds, a risk assessment for each vehicle that assists CBP Offices at primary booths in determining whether to allow a vehicle to cross without further inspection or to send the vehicle for secondary evaluation."[22]ATS-L stores vehicle registration information (year, make, model, and Vehicle Identification Numbers), registered owner information (name, date of birth, and address) for U.S.-plated vehicles, and biographical

[17] *Id*. at 4.
[18] *Id*. at 7.
[19] *Id*. at 8.
[20] *Id*.
[21] *Id*. at 5-6.
[22] Privacy Office, Dep't of Homeland Sec., *Privacy Impact Assessment for the Automated Targeting System*, Aug. 3, 2007 [hereinafter "ATS Privacy Impact Assessment"], 5-6 *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_atsupdate.pdf.

information of all vehicle occupants.[23] CBP then cross-references this information against previous crossing records and other government data sources.[24]

According to CBP, ATS-P "is a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals and, in some cases, other persons who pose a higher risk of violating U.S. law."[25] ATS-P also vets non-immigrant and immigrant visa applications for the State Department and monitors for "potential visa overstay candidates."[26]

Since its inception, ATS and ATS modules have gradually expanded to include a plethora of information relating to an expansive group of individuals. ATS now applies broadly to "[p]ersons who may pose a threat to the United States,"[27] as well as

> A. Persons, including operators, crew, and passengers, who seek to, or do in fact, enter, exit, or transit through the United States or through other locations where CBP maintains an enforcement or operational presence by land, air, or sea.
> B. Crew members traveling on commercial aircraft that fly over the United States.
> C. Persons who engage in any form of trade or other commercial transaction related to the importation or exportation of merchandise, including those required to submit an Importer Security Filing.
> D. Persons who are employed in any capacity related to the transit of merchandise intended to cross the United States border.
> E. Persons who serve as booking agents, brokers, or other persons who provide information on behalf of persons seeking to enter, exit, or transit through the United States, or on behalf of persons seeking to import, export, or ship merchandise through the United States.
> F. Owners of vehicles that cross the border.
> G. Persons whose data was received by the Department as the result of memoranda of understanding or other information sharing agreement or arrangement because the information is relevant to the border security mission of the Department.
> H. Persons who were identified in a narrative report, prepared by an officer or agent, as being related to or associated with other persons who are alleged to be involved in, who are suspected of, or who have been arrested for violations of the laws enforced or administered by DHS.[28]

Under these criteria, it is conceivable that the majority of Americans are currently included in these modules and subject to monitoring and risk-based evaluation by CBP. Moreover, ATS contains an

[23] ATS Privacy Impact Assessment at 6.
[24] *Id*. at 5
[25] *Id*. at 6.
[26] *Id*.
[27] 77 Fed. Reg. 30299.
[28] *Id*.

endless collection of individually identifiable data, including but not limited to race, age, gender, nationality, citizenship, and

> Name; Addresses (home, work, and/or destination, as appropriate); Telephone and fax numbers; Tax ID number (e.g., Employer Identification Number (EIN) or Social Security Number (SSN), where available); place of birth; Country of Residence; Alias; Physical characteristics, including biometrics where available (e.g., height, weight, race, eye and hair color, scars, tattoos, marks, fingerprints); Familial relationships and other contact information; Property information; Occupation and employment information; Biographical and biometric information from or associated with online immigrant and nonimmigrant visa applications, including (as available): U.S. sponsor's name, address, and phone number ,U.S. contact name, address, and phone number, Employer name, address, and phone number, Email address, IP Address, applicant ID, Marital Status, Alien number, Social Security Number ,Tax Identification Number, Organization Name, U.S. Status Income information for Joint Sponsors, Education, military experience, relationship information Responses to vetting questions pertaining to admissibility or eligibility; Information from documents used to verify the identity of individuals (e.g., driver's license, passport, visa, alien registration, citizenship card, border crossing card, birth certificate, certificate of naturalization, re-entry permit, military card) including the: type, number, date of issuance, place of issuance.[29]

The system contains travel information pertaining to individuals, including:

> The combination of license plate, Department of Motor Vehicle (DMV) registration data and biographical data associated with a border crossing; Information derived from an ESTA application including responses to vetting questions pertaining to admissibility (where applicable); Travel itinerary; Date of arrival or departure, and means of conveyance with associated identification (e.g., Vehicle Identification Number, year, make, model, registration).
>
> Passenger Name Record (PNR): 1. PNR record locator code 2. Date of reservation/issue of ticket 3. Date(s) of intended travel 4. Name(s) 5. Available frequent flier and benefit information (i.e., free tickets, upgrades) 6. Other names on PNR, including number of travelers on PNR 7. All available contact information (including originator of reservation) 8. All available payment/billing information (e.g., credit card number) 9. Travel itinerary for specific PNR 10. Travel agency/travel agent 11. Code share information (e.g., when one air carrier sells seats on another air carrier's flight) 12. Split/divided information (e.g., when one PNR contains a reference to another PNR) 13. Travel status of passenger (including confirmations and check-in status) 14. Ticketing information, including ticket number, one way tickets and Automated Ticket Fare Quote (ATFQ) fields 15. Baggage information 16. Seat information, including seat number 17. General remarks including Other Service Indicated (OSI), Special Service Indicated (SSI) and Supplemental Service Request (SSR) information 18. Any collected APIS information (e.g., Advance Passenger Information (API)) that is initially captured by an air carrier within its PNR, such as passport number, date of birth and gender) 19. All historical changes to the PNR listed in numbers 1 to 18.[30]

CBP claims that a passenger's PNR "likely will not include information for all possible categories." PNR can also include "information that could directly indicate the racial or ethnic origin,

[29] *Id*. at 30299-300.
[30] *Id*. at 30300.

political opinions, religious or philosophical beliefs, trade union membership, health, or sex life of the individual."[31]

ATS is the originating source for some of these records, including the Passenger Name Records, Department of Motor Vehicle registration and biographical data associated with border crossing.[32] For other records, CBP states that ATS "ingests" and/or accesses information from at least 30 other databases.[33]

Incredibly, CBP proposes to exempt this massive database containing detailed, sensitive personal information from well-established Privacy Act safeguards. It is inconceivable that the drafters of the Privacy Act would have permitted a federal agency to propose a massive profiling system on U.S. citizens and be granted broad exemptions from Privacy Act obligations. Consistent and broad application of Privacy Act obligations are the best means of ensuring accuracy and reliability of the data used in a system that profoundly affects millions of individuals as they travel to, from, and throughout the United States on a daily basis.

III. Data Concerning Race, Ethnicity, Political Opinions, or Religious Beliefs May be Used in ATS "Risk Assessments"

ATS is equipped to make adverse "risk assessment" determinations based on race, ethnicity, gender, political and religious beliefs. As mentioned above, ATS contains PNR data. These records can include up to 19 categories of data. Besides information such as name, credit card information, and travel dates, PNR can also include "information that could directly indicate the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life of the individual."[34] CBP claims that it "employs an automated system that filters certain of these terms and only uses this information in exceptional circumstances where the life of an individual could be imperiled or

[31] *Id*.
[32] ATS Privacy Impact Assessment at 3.
[33] *Id*.
[34] 77 Fed. Reg. 30300.

seriously impaired."[35] It is hard to imagine the "exceptional circumstance" under which CBP needs to use information relating to an individual's sex life. It is even more disturbing to imagine what source(s) CBP would use to gather that information. Moreover, because information such as race, nationality, ethnic origin, political and religious beliefs are included in ATS, there is the distinct possibility that travelers will be discriminated against based upon these factors. This information should never be used to assess an individual's purported "risk" for terrorist activities, or for discriminatory purposes. In fact, various U.S. laws expressly proscribe discrimination based on age, sex, race, gender, religion, or political beliefs.[36] ATS, however, admittedly collects information pertaining to race and can use it for discriminatory purposes. ATS has the capability to infringe upon the civil rights of millions of individuals; therefore CBP absolutely must cease collecting this information.

Although the proposed rule would grant individuals access to amend their PNR data that includes this information,[37]that does not militate against possible discrimination. Therefore, CBP should remove information detailing racial, ethnic origin, political opinions, religious, philosophical beliefs, trade union membership, health and sex life from the PNR and ATS.

IV. The Privacy Impact Assessment Reveals ATS's Numerous Privacy Risks and Underscores the Problems of Granting the Privacy Act Exemptions the Agency Seeks

The ATS Privacy Impact Assessment does nothing to ameliorate concerns about the impact of the Automated Targeting System. In fact, the Privacy Impact Assessment makes clear that the program

[35] *Id*.
[36] *See, e.g.*, Civil Rights Act of 1964 § 201, 42 U.S.C. § 2000a (2006); Civil Rights Act of 1964 § 703, 42 U.S.C. § 2000e-2 (2006); Patsy Takemoto Mink Equal Opportunity in Education Act § 901, 20 U.S.C. § 1681 (2006); Rehabilitation Act of 1973 § 504, 29 U.S.C. §794 (2006); Religious Freedom Restoration Act of 1993, 42 U.S.C.§§ 2000bb-bb4 (2006). *See also United States v. Carolene Products Co.*, 304 U.S. 144, 153 n.4 (1938) ("[P]rejudice against discrete and insular minorities may be a special condition, which tends seriously to curtail the operation of those political processes ordinarily to be relied upon to protect minorities, and which may call for a correspondingly more searching judicial inquiry.").
[37] 77 Fed. Reg. 30434.

should not continue. The assessment sets out the various privacy risks associated with "access to datasets used by and stored in ATS,"[38] yet does nothing to solve them.

For example, ATS is accessible over web-based "DHS infrastructure or remotely through secure encrypted devices with one-factor authentication."[39] Certain ATS modules are also "accessible through secure-encrypted mobile devices."[40] CBP needs to implement multifactor authentication for the expansive ATS database. As already explained, ATS collects and retains troves of sensitive biographical, financial, health, education, and occupation records. CBP insufficiently safeguards against unauthorized access by solely requiring one-factor authentication to this information. Government databases are frequently hacked and compromised.[41] One-factor authentication increases the likelihood that ATS can be compromised.

CBP also acknowledges the risks of unauthorized access to ATS for "unapproved or inappropriate" purposes or sharing. CBP claims that requiring supervisor approval and expressly defining the nature of "access to or sharing of ATS information" mitigates these risks. This, however, does not militate against privacy risks because CBP grants ATS users an extremely broad basis for accessing ATS information. According to CBP, ATS access "is limited to those individuals with a need to know in order to carry out their official duties." But because ATS information is accessible to countless individuals for a vast array of purposes,[42] limiting access on a "need to know" basis becomes meaningless.

These are just a few of the numerous vulnerabilities that the Privacy Impact Assessment acknowledges, but does not solve. The Privacy Impact Assessment makes clear that ATS does not defend

[38] ATS Privacy Impact Assessment at 2.
[39] *Id*. at 9.
[40] *Id*.
[41] *See, e.g.*, Matt Liebowitz, *Iranian 'Cyber Warriors Team' Takes Credit for NASA Hack*, MSNBC.COM, May 22, 2012, http://www.msnbc.msn.com/id/47522497/ns/technology_and_science-security/t/iranian-cyber-warriors-team-takes-credit-nasa-hack/#.T9pOHOJYs5O; Lisa Rein, *For Commerce Unit Hit by Computer Virus, Hardship of Being Unplugged Has Upside*, WASHINGTON POST, Apr. 9, 2012, *available at* http://www.washingtonpost.com/politics/for-agency-a-loss-of-technology-has-had-down--and-upsides/2012/04/08/gIQAvpAY5S_story.html?hpid=z3&tid=sm_twitter_washingtonpost; Nicole Perlroth, *Hackers Step Up Attacks After Megaupload Shutdown*, THE NEW YORK TIMES, Jan. 24, 2012, *available at* http://bits.blogs.nytimes.com/2012/01/24/hackers-step-up-attacks-after-megaupload-shutdown/.
[42] 77 Fed. Reg. 30300-302.

against unauthorized access, and that the database should therefore be suspended until CBP properly protects the PII within the system.

V. CBP Must Provide Transparency in the ATS Algorithm and Must Make Public The Factors Used for ATS "Risk Assessments"

Little information is known about ATS algorithms used to determine which individuals will be scrutinized upon entering, exiting, or traveling throughout the United States. All of the key characteristics of the system – including the assessment, the basis for the assessment, the rules that apply, and the "targeting activities" – are secret. This is not transparency. ATS evaluates pre-existing information on individuals coming in and leaving the country "with patterns identified as requiring additional scrutiny."[43] CBP does not provide a clear explanation as to how these patterns are recognized and what they are composed of, instead elaborating that the patterns "are based on CBP officer experience, analysis of trends of suspicious activity, and raw intelligence corroborating those trends."[44] It is not clear what activity is determined to be suspicious and how much weight it is given when being evaluated by ATS.

ATS operates via automated data processing. This troubling practice will ultimately violate important personal rights as enumerated in such well-established privacy provisions as Article 15.1 of the 1995 EC Directive on Data Protection. The directive, which provoked many European countries to enact provisions along the lines of article 15.1,[45] states that "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."[46] In particular, Article 12.1 of the EU Data Protection Directive also grants individuals the right to obtain "the logic," *i.e.* the algorithm, of the processing of personal data.

---

[43] 77 Fed. Reg. 30433.
[44] *Id*.
[45] Lee A. *Bygrave, Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUTER LAW & SOC. REP. 17, 18 (2001).
[46] Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 15, 1995 O.J. (L 281) 11.23.1995 (EC).

ATS would directly violate this right because the decision of which persons should undergo additional screening is entirely automated. CBP must ensure transparency and make public the algorithm that it has established to assign "risk-based" profiles to individuals so as to not further violate personal rights.

VI. CBP Proposes Broad Exemptions for the Automated Targeting System, Thus Contravening the Intent of the Privacy Act of 1974

CBP continues to broaden previously established exemptions for ATS, which contravenes the intent of the Privacy Act of 1974. CBP argues for these broad exemptions because they are of a "law enforcement" nature.[47] While CBP maintains the discretion to make decisions regarding ATS-record access requests, they will provide access and amendment to PNR, importer security filing information, and "any records that were ingested by ATS where the source system of records already provides access and/or amendment under the Privacy Act."[48] As mentioned above, CBP will not provide individuals with access to the following records:

> the targeting rules, the responses to rules, case events, law enforcement and/or intelligence data, reports, projects developed by CBP analysis that may include public source and/or classified information, information obtained through memorandum of understanding or other arrangements because the information is relevant to the border security mission of the Department, or records exempted from access by the system from which ATS ingested or accessed the information.[49]

CBP claims that certain requirements of the Privacy Act for DHS/CBP-006-Automated Targeting System (ATS) System of Records are exempted based upon standard law enforcement, immigration, and intelligence activities.[50] Furthermore, CBP is claiming exemptions in order:

> to preclude subjects of these activities from frustrating these processes, to avoid disclosure of activity techniques; to protect the identities and physical safety of confidential informants and law enforcement personnel; to ensure DHS' ability to obtain information from third parties and other

[47] 75 Fed. Reg. 30433, EPIC, *Comments on Docket Nos. DHS-2007-0042; Notice of Privacy Act System of Records: U.S. Customs and Border Protection, Automated Targeting System, System of Records and DHS-2007-0043: Notice of Proposed Rulemaking: Implementation of Exemptions; Automated Targeting System* (Sept. 5, 2007) [hereinafter "EPIC Comments 0042-0043"], *available at* http://epic.org/privacy/travel/ats/epic_090507.pdf.
[48] 75 Fed. Reg. 30433.
[49] 75 Fed. Reg. 30434.
[50] *Id*.

> sources; to protect the privacy of third parties; and to safeguard officially classified and/or controlled information. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.[51]

Specifically, CBP proposes to exempt: "5 U.S.C. 552(a)(c)(3) and (4); (d)(1), (2), (3), and (4); e(1), (2), (3), (4)(G) through (I), (e)(5), and (8); (f), and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2)." These provisions of the Privacy Act ensure that:

- an agency must give individuals access to the accounting of disclosure of their records[52];
- any agency or individual to whom the records are disclosed must also receive "any correction or notation of dispute"[53];
- an individual may request access to records an agency maintains about him or her, as well as have a copies made[54];
- the agency must permit the individual to amend a record about him or her and acknowledge the request in writing within 10 days, as well as timely correct the record if necessary or provide a reason for refusal of the proposed amendment, as well as allow a review of the refusal[55];
- an agency must make notes of requested amendments within the records[56];
- an agency must collect records "about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President"[57];
- an agency must "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs"[58];
- each individual must be informed whom the agency asks to supply information[59];
- an agency must publish the establishment or revision of the notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access, contest content, and learn the categories of sources or records in the system[60];
- assure that all records used by the agency in making determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness[61];

[51] 75 Fed. Reg. 30434.
[52] 5 U.S.C. §552a(c)(3).
[53] 5 U.S.C. §552a(c)(4).
[54] 5 U.S.C. §552a(d)(1).
[55] 5 U.S.C. §552a(d)(2), (d)(3).
[56] 5 U.S.C. §552a(d)(4).
[57] 5 U.S.C. §552a(e)(1).
[58] 5 U.S.C. §552a(e)(2).
[59] 5 U.S.C. §552a(e)(3).
[60] 5 U.S.C. §552a(e)(4)(G), (H), (I).
[61] 5 U.S.C. §552a(e)(5).

- make a reasonable effort to notify an individual when a record about him or her is made available to another individual when it is a matter of public record[62];
- the agency shall promulgate rules establishing procedures that notify an individual in response to record requests pertaining to him or her, including "reasonable times, places, and requirements for identifying an individual", instituting disclosure procedures for medical and psychological records, create procedures, review amendment requests, as well as determining the request, the status of appeals to denial of requests, and establish fees for record duplication, excluding the cost for search and review of the record[63];
- an individual may bring civil action in U.S. district court against an agency within two years of the date of the cause of action or within two years of the date of discovery by an individual of misrepresentation by the agency, when it makes a determination not to amend an individual's record according to his or her request or fails to maintain the record with accuracy, timeliness, relevance, and completeness, adversely effecting the individual[64];
- the court may order the agency to amend the individual's record as requested, the court may assess reasonable attorney fees and other litigation costs, as well as enjoin the agency from withholding records[65].

CBP egregiously attempts to circumvent the intent of the Privacy Act in order to create a massive database that lacks accountability. CBP must limit its exemption from Privacy Act Subsection (e)(8). It is unknown what value would be gained by exempting the agency from its Privacy Act obligation to make reasonable efforts to serve notice on an affected individual, especially after the matter has become public record.[66] This broad exception only serves to increase the secrecy of the database. CBP claims that these notification and access provisions, if implemented, may put entities on notice that they are being investigated, thereby hindering their investigative efforts.[67]

While EPIC recognizes the need to withhold notice during the period of the investigation, individuals should be able to know, after an investigation is completed or made public, the information stored about them in the system. Access to records of a completed investigation, with appropriate redactions to protect the identities of witnesses and informants, would provide individuals and entities with the right to address potential inaccuracies. And because the investigations have already been

[62] 5 U.S.C. §552a(e)(8).
[63] 5 U.S.C. §552a(f)(1), (2), (3), (4), (5).
[64] 5 U.S.C. §552a(g)(1)(A), (B), (C), (D).
[65] 5 U.S.C. §552a(g)(2)(A), (B), 3(A), (B), 5.
[66] 5 U.S.C. §552(a)(e)(8).
[67] 77 Fed. Reg. 30435.

completed, CBP's law enforcement purposes would not be undermined. Privacy rights of entities and their individual members would be sufficiently protected.

When Congress enacted the Privacy Act in 1974, it sought to restrict the amount of personal data that Federal agencies were able to collect, and furthermore, required agencies to be transparent in their information practices.[68] In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that: "in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary … to regulate the collection, maintenance, use, and dissemination of information by such agencies." [69]

By proposing to exempt ATS from subsection (g) of the Privacy Act, CBP effectively denies individuals of judicially enforceable rights of access to their records or correction of erroneous information in such records. Therefore CBP must re-instate civil remedies for individuals against whom the agency has failed to comply with its obligations under the Privacy Act.

The Privacy Act is intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. By allowing CBP to encroach on an individual's right to access and amend their information, CBP violates the intent of the Privacy Act. If ATS is allowed these exemptions, then the government fails to ensure the reliability of the data, provide citizens with access to their personal data, or opportunities to correct inaccurate or incomplete data. These failures are especially significant because ATS will affect anyone or anything traveling to, from, or throughout the United States.

VII. Proposed Routine Uses G, H, I, J, and M Remove Privacy Act Safeguards by Disclosing Records to Foreign Agencies, Multilateral Governmental Organizations, and other Foreign Entities That are Not Subject to the Privacy Act

Proposed Routine Use G would permit the agency to disclose information:

> [t]o appropriate federal, state, tribal, local, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violation of, or for

[68] S. Rep. No. 93-1183 at 1 (1974).
[69] *Doe v. Chao*, 540 U.S. 614, 618 (2004).

> enforcing or implementing, a statute, rule, regulation, order, or license, where CBP believes the information would assist enforcement of applicable civil or criminal law;[70]

Proposed Routine Use H would permit the agency to disclose information:

> [t]o federal and foreign government intelligence or counterterrorism agencies or components where DHS becomes aware of an indication of a threat or potential threat to national or international security, or to assist in anti-terrorism efforts;[71]

Proposed Routine Use I would permit the agency to disclose information:

> [t]o an organization or person in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, or where the information is relevant to the protection of life, property, or other vital interests of a person;[72]

Proposed Routine Use J would permit the agency to disclose information:

> [t]o appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk;[73]

Proposed Routine Use M would permit the agency to disclose information:

> [t]o appropriate federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations where CBP is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance ATS;[74]

The provisions in these Routine Uses that would permit CBP to disclose information to foreign agencies, multilateral governmental organizations, or foreign persons in the public or private sector, must be removed. The Privacy Act only applies to records maintained by United States government agencies.[75] Releasing information to foreign entities does not protect individuals covered by ATS from Privacy Act violations. CBP does not have jurisdiction over foreign agents, therefore, the provisions in these Routine Uses that would permit CBP to disclose information to foreign or multilateral entities must be removed.

[70] 77 Fed. Reg. 30302.
[71] 77 Fed. Reg. 30302.
[72] 77 Fed. Reg. 30302.
[73] 77 Fed. Reg. 30302.
[74] 77 Fed. Reg. 30302.
[75] 5 U.S.C. § 552a(b).

VIII. Routine Uses G, H, I, M, and N Contravene the Legislative Intent of the Privacy Act

Proposed Routine Use N would permit the agency to disclose information:

> [t]o the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy. [76]

The limitations on disclosure in proposed Routine Uses G, H, I, M, and N are too broad to have any substantive effect, create opportunities for violations of statutory rights, and go against the legislative intent of the Privacy Act. As it stands, these Routine Uses directly contradict Congressman William Moorhead's testimony that the Privacy Act was "intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes."[77]

Under proposed Routine Use G, CBP can disclose any information where it believes information would assist the enforcement of applicable laws.[78] This ill-defined limitation creates opportunities to arbitrarily disclose private information to entities that are not subject to the Privacy Act, potentially including any information that might assist in law enforcement. This criterion must be clarified in order to prevent abuse.

The limitation on disclosure as proposed in Routine Use H is too broad to have a substantive effect and therefore creates numerous opportunities for violations of statutory rights. Routine Use H would permit CBP to disclose information after indication of a threat or potential threat, a category that would create opportunities to arbitrarily disclose private information on the basis of a possible threat without concrete evidence establishing a threat or potential threat.

---

[76] 77 Fed. Reg. 30302.
[77] Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy, 1031 (1976).
[78] 77 Fed Reg. 30302.

Routine Use I permits disclosure of information pertinent to a law enforcement investigation. This is an extremely broad limitation and the definition of "appropriate" must be made clear. Otherwise, information may be arbitrarily disclosed at the discretion of a lone CBP officer. This murky Routine Use creates opportunities for violations of statutory rights and goes against the legislative intent of the Privacy Act.

Under the limitation on disclosure in proposed Routine Use M, CBP can disclose any information for the testing of new technology designed to enhance ATS. This ill-defined limitation creates opportunities to arbitrarily disclose private information to entities that are not subject to the Privacy Act. The definition of "new technology" and "testing" must be clarified. As it stands this Routine Use creates the opportunity for abuses of discretion and necessary disclosure merely to test any technology that CBP sees fit.

The phrase "when disclosure is necessary to preserve confidence in the integrity of DHS"[79] in Routine Use N is discordant with the Privacy Act because it gratuitously puts the face of the agency above an individual's right to privacy. The term "necessary" is overly ambiguous; CBP could take advantage of this criterion to unduly influence its image. CBP should remove this phrase from the proposed Routine Use because creating a category that is too broad can easily lead to the abuse of privacy rights of individuals whose data has been gathered and stored by CBP.

IX. CBP's Lack of Opportunity to Review Public Comment Violates the Administrative Procedure Act and Therefore the Routine Uses and Proposed Exemptions Should Not Be Implemented Without Public Comment Review

A. CBP's Proposed Routine Uses and Exemptions Will Have a Substantial Effect on Members of the Public and Therefore Require Public Notice and Comment

The Privacy Act requires each agency to "at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit

[79] 77 Fed. Reg. 30302.

written data, views, or arguments to the agency."[80] Paragraph (4)(D) of the subsection referenced above, subsection (e), refers to "each routine use of the records contained in the system, including the categories of users and the purposes of such use."[81]

In addition to the Privacy Act's Federal Register public notice requirement, CBP is also obligated under the Administrative Procedure Act ("APA") to provide notice and comment on the proposed updates to the system of records because the system of records' "substantive effect is sufficiently grave so that notice and comment are needed to safeguard the policies underlying the APA."[82] The SORN published by CBP also states "[e]lsewhere in the federal register, the Department of Homeland Security is concurrently issuing a Notice of Proposed Rulemaking exempting this system of records from certain provisions of the Privacy Act."[83] The substantive effect of the proposed routine uses and exemptions within CBP's system of records are "sufficiently grave" because they "impose directly and significantly upon so many members of the public."[84] CBP's system of records applies to a broad and poorly-defined category of individuals, including "owners of vehicles that cross the border... persons who may pose a threat to the United States," and "persons, including operators, crew, and passengers, who seek to, or do in fact, enter, exit, or transit through the United States or through other locations where CBP maintains an enforcement or operational presence by land, air, or sea."[85] The system also significantly impacts with whom personal information will be shared. Over half of the proposed routine uses would permit CBP to disclose information to either foreign or international agencies, third party individuals, the news media, or the public, none of whom are subject to "the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees" or contractors.[86] The proposed routine uses and

[80] 5 U.S.C. § 552a(e)(11).
[81] *Id*. at (e)(4)(D).
[82] *Electronic Privacy Information Center v. U.S. Dep't. of Homeland Sec., 653 F.3d 1, 5- 6 (D.C.Cir. 2011) (rehearing en banc denied)(quoting Lamoille Valley R.R.Co. v. ICC, 711 F.2d 295, 328 (D.C.Cir.1983));* Administrative Procedure Act, 5 U.S.C. §§ 553 (b) - (c) (2006).
[83] 77 Fed. Reg. 30297.
[84] *Electronic Privacy Information Center v. U.S. Dep't. of Homeland Sec.,* 653 F.3d at 6.
[85] 77 Fed. Reg. 30299.
[86] *Id*. at 30301 - 02.

exemptions create "sufficiently grave" privacy risks to members of the public, and accordingly require notice and comment.

B. CBP Must Consider and Respond to Public Comments It Receives Before Implementing The Proposed Routine Uses and Exemptions

Following the required notice and comment period, the APA states that "[a]fter consideration of the relevant matter presented, the agency shall incorporate in the rules adopted a concise general statement of their basis and purpose."[87] Indeed, the "essential purpose of those [notice and comment] provisions is the generation of comments that will permit the agency to improve its tentative rule"[88] and to give the agency "the opportunity 'to educate itself on the full range of interests the rule affects'."[89] Additionally, it is well established that agencies must provide a rationale for their decision-making processes by "responding to those comments that are relevant and significant."[90]

CBP's SORN invites the public to "submit comments on or before June 21, 2012," which is also the same day the new routine uses go into effect.[91] Moreover, the deadline to submit comments for the proposed exemptions is June 22, 2012,[92] one day after the system goes into effect.[93] By failing to consider the public comments it receives in response to the substantial privacy risks posed by the proposed routine uses and exemptions, CBP violates the APA requirement that agencies consider "the relevant matter[s] presented."[94]

---

[87] 5 U.S.C. § 553(c).
[88] *Am. Fed'n of Labor & Cong. of Indus. Organizations v. Donovan*, 757 F.2d 330, 337 (D.C. Cir. 1985) (quoting *Am. Fed'n of Labor & Cong. of Indus. Organizations v. Donovan,* 582 F. Supp. 1015, 1024 (D.D.C. 1984)).
[89] *Louis v. U.S. Dept. of Labor*, 419 F.3d 970, 976-77 (9th Cir. 2005) (quoting *Alcaraz v. Block,* 746 F.2d 593, 611 (9th Cir. 1984)).
[90] *Grand Canyon Air Tour Coal v. FAA,* 154 F.3d 455, 468 (D.C.Cir. 1998); *Cement Kiln Recycling Coalition v. E.P.A.,* 493 F.3d 207, 225 (D.C. Cir. 2007); *Interstate Natural Gas Ass'n of America v. F.E.R.C.,* 494 F.3d 1092, 1096 (D.C. Cir. 2007); *Int'l Fabricare Inst. V. U.S. EPA,* 972 F.2d 384, 389 (D.C.Cir. 1992).
[91] 77 Fed. Reg. 30297.
[92] 77 Fed. Reg. 30433.
[93] 77 Fed. Reg. 30297.
[94] 5 U.S.C. § 553(c).

C. CBP's Proposed Routine Uses Must Fall on Procedural Grounds Due to CBP's Inadequate Public Comment Review

CBP's notice and comment procedure concerning the proposed routine uses is inadequate because the agency does not afford itself opportunity to review the public comments it receives. Additionally, retroactively applying the proposed exemptions to ATS a day after the updated system goes into effect would be equivalent to acting without considering and responding to public comments. CBP effectively denies the public any meaningful opportunity to comment on ATS because the agency fails to consider "the relevant matter[s] presented."[95] One of the core principles of the APA is public participation in the rulemaking process. Here, CBP attempts to circumvent this democratic process by failing to consider and address public comments.

Consequently, "[i]f the agency fails to provide this notice and opportunity to comment or the notice and comment period are inadequate, the 'regulation must fall on procedural ground and the substantive validity of the change accordingly need not be analyzed'."[96] Therefore the proposed rule must fall on procedural grounds. The proposed Routine Uses and exemptions must not be implemented without the agency reviewing and considering public comment; failure to do so is unlawful.[97]

X. Conclusion

For the foregoing reasons, the Automated Targeting System, which establishes secret profiles on individuals absent Privacy Act safeguards, is contrary to the core purpose of the federal Privacy Act. We urge the agency to suspend this program. If the program goes forward, CBP must revise its Privacy Act notice for the Automated Targeting System to: 1) provide individuals judicially enforceable rights of access and correction; 2) limit the collection and distribution of information to only those necessary for the screening process, and 3) substantially limit the routine uses of information. EPIC anticipates the

---

[95] *Id*.
[96] *Public Citizen, Inc. v. Mineta,* 427 F.Supp.2d 7, 12 (D.D.C. 2006) (quoting *AFL-CIO v. Donovan,* 757 F.2d 330, 338 (D.C.Cir. 1985)). *See also Stainback v. Mabus,* 671 F. Supp.2d 126, 135 (D.D.C. 2009); *Steinhorst Associates v. Preston,* 572 F.Supp.2d 112, 124 n. 13 (D.D.C. 2008); *National Ass'n of Home Builders v. U.S. Army Corps of Engineers,* 453 F. Supp. 2d 116, 123 (D.D.C. 2006).
[97] 5 U.S.C. 706(2)(D).

agency's specific and substantive responses to each of these proposals.

Additionally, as discussed above in detail, the proposed Routine Uses and exemptions are unlawful because they are "without observance of procedure required by law," and should be withdrawn. If the agency fails to take account of EPIC's comments in this matter, the organization will pursue all available options to seek suspension of the program.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Open Government Fellow

Kimberly Koopman
EPIC Law Clerk

John Sadlik
EPIC Law Clerk