epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF HOMELAND SECURITY

Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Immigration and Customs Enforcement-016 FALCON Search and Analysis System of Records

[Docket Nos. DHS-2017-0001; 2017-0002]

June 5, 2017

By notice published May 4, 2017 the Department of Homeland Security ("DHS") proposes several Privacy Act exemptions to the FALCON Search and Analysis System of Records ("FALCON" or "Database").[1] The Database includes detailed, personal information on many individuals who are connected Immigration and Customs Enforcement ("ICE") investigations. This includes individuals suspected of crimes, individuals connected to those suspected of crimes, ICE and Customs and Border Protection ("CBP") personnel, individuals suspected of suspicious or illegal activity, individuals who report suspicious or illegal activity, and government personnel associated with official requests for ICE assistance. The information contained in FALCON includes social security numbers, financial data, call records, social media data, Internet Service Provider data (including domain name, IP address, and subscriber data), and law enforcement records.[2]

[1] *Notice of a New Privacy Act system of records,* 82 Fed. Reg. 20,905 (May 4, 2017) (hereafter "FALCON SORN"); *Notice of proposed rulemaking,* 82 Fed. Reg. 20,844 (May 4, 2017) (hereafter "FALCON NPRM").
[2] FALCON SORN at 20,907-908.

The agency has indicated their intention to exempt themselves from several significant provisions of the Privacy Act. EPIC submits these comments to (1) underscore the substantial privacy and security issues raised by the database; (2) recommend that DHS withdraw unlawful and unnecessary proposed routine use disclosures; and (3) to urge DHS to significantly narrow their Privacy Act exemptions.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and protect privacy, the First Amendment, and constitutional values.[3] EPIC has a particular interest in preserving the right of people to engage in First Amendment protected activities without the threat of government surveillance.

I. Purpose and Scope of FALCON

FALCON is a tool used by ICE to "search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws."[4] FALCON data consists of data obtained from ICE, DHS, and other government databases as well as information that is uploaded on an *ad hoc* basis.[5] The Database contains information on individuals who have had an encounter with DHS "of a law enforcement nature" and contains substantial amounts of personally identifiable information.[6]

The FALCON database allows users to create a searchable index of information that can be searched by ICE agents with tools to analyze and visualize data and to identify relationships.[7] Additionally, trade data can also be accessed by foreign government personnel on a case-by-case

[3] EPIC, *About EPIC* (2016), https://epic.org/epic/about.html.
[4] FALCON SORN at 20,905.
[5] *Id.*
[6] *Privacy Impact Assessment Update for the FALCON Search & Analysis System*, DHS, Oct. 11, 2016 (hereafter "FALCON PIA").
[7] *Id.* at 1.

basis.[8] Individuals with access to the Database can upload or input information, search and conduct saved searches, conduct analysis, and share or publish data.[9] However, in response to a recent Freedom of Information Act request for rules and restrictions for use of FALCON the agency responded that "no such documents had been found."[10]

While the database is intended to contain information on those who have had contact of a law enforcement nature with DHS, the agency has stated that the population of individuals whose data is collected will evolve over time.[11]

II. The FALCON Database Would Maintain a Massive Amount of Personal, Sensitive Information About a Wide Variety of Individuals

a. Categories of Records in the DHS Database Are Virtually Unlimited

According to the FALCON system of records notice ("SORN"), the Database will likely include an exorbitant amount of personal information about an expansive array of individuals. The categories of records contained in the FALCON Database represent a wealth of sensitive information that should be afforded the highest degree of privacy and security protections, such as health,[12] financial,[13] and education[14] records; Social Security Numbers;[15] and individuals' photographs or images.[16] Federal contractors, security experts, and EPIC have argued to the U.S.

---

[8] *2016 Data Mining Report to Congress,* DHS, Apr. 2017 (hereafter "2016 Data Mining Report.")
[9] FALCON PIA at 3.
[10] Spencer Woodman, *Palantir Enables Immigration Agents to Access Information from the CIA,* The Intercept, Mar. 17, 2017, https://theintercept.com/2017/03/17/palantir-enables-immigration-agents-to-access-information-from-the-cia/.
[11] FALCON PIA at 10.
[12] *See* Heath Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 42 U.S.C.).
[13] *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered section of 12 and 15 U.S.C.).
[14] *See* Family Educational Rights and Privacy Act, 20 U.S.C. §1232g (2012).
[15] *See* Driver's Privacy Protection Act, 18 U.S.C. § 2725(4) (defining "highly restricted personal information" to include "social security number").
[16] *Id*. § 2725(4) (defining "highly restricted personal information" to include "individual's photograph or image").

Supreme Court that much of this information simply should not be collected by the federal government.

In *NASA v. Nelson*,[17] the Supreme Court considered whether federal contract employees have a Constitutional right to withhold personal information sought by the government in a background check. EPIC filed an amicus brief, signed by 27 technical experts and legal scholars, siding with the contractors employed by the Jet Propulsion Laboratory ("JPL").[18] EPIC's brief highlighted problems with the Privacy Act, including the "routine use" exception, security breaches, and the agency's authority to carve out its own exceptions to the Act.[19] EPIC also argued that compelled collection of sensitive data would place at risk personal health information that is insufficiently protected by the agency.[20] The Supreme Court acknowledged that the background checks implicate "a privacy interest of Constitutional significance" but stopped short of limiting data collection by the agency, reasoning that the personal information would be protected under the Privacy Act.[21]

That turned out not to be true. Shortly after the Court's decision, NASA experienced a significant data breach that compromised the personal information of about 10,000 employees, including Robert Nelson, the JPL scientist who sued NASA over its data collection practices.[22] The JPL-NASA breach is a clear warning about why DHS should narrow the amount of sensitive data collected. Simply put, the government should not collect so much data; to do so unquestionably places people at risk.

---

[17] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).
[18] Amicus Curiae Brief of EPIC, *Nat'l Aeronautics & Space Admin. v. Nelson*, No. 09-530 (S.Ct. Aug. 9, 2010), https://epic.org/amicus/nasavnelson/EPIC_amicus_NASA_final.pdf.
[19] *Id*. at 20-28
[20] *Id*.
[21] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 147 (2011).
[22] Natasha Singer, *Losing in Court, and to Laptop Thieves, in a Battle With NASA Over Private Data*, N.Y. TIMES (Nov. 28, 2012), http://www.nytimes.com/2012/11/29/technology/ex-nasa-scientists-data-fears-come-true.html.

Given the recent surge in government data breaches, the vast amount of sensitive information contained in the FALCON Database faces significant risk of compromise. According to a recent report by the U.S. Government Accountability Office ("GAO"), "[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive."[23] This is illustrated by the 2015 data breach at OPM, which compromised the background investigation records of 21.5 million individuals.[24] Also in 2015, the Internal Revenue Service ("IRS") reported that approximately 390,000 tax accounts were compromised, exposing Social Security Numbers, dates of birth, street addresses, and other sensitive information.[25] In 2014, a data breach at the U.S. Postal Service exposed personally identifiable information for more than 80,000 employees.[26]

The latest series of high-profile government data breaches indicates that federal agencies are incapable of adequately protecting sensitive information from improper disclosure. Indeed, GAO recently released a report on widespread cybersecurity weaknesses throughout the executive branch, aptly titled "Federal Agencies Need to Better Protect Sensitive Data."[27] According to the report, a majority of federal agencies, "have weaknesses with the design and implementation of information security controls …."[28] In addition, most agencies "have weaknesses in key controls such as those for limiting, preventing, and detecting inappropriate access to computer resources and managing the configurations of software and hardware."[29] The GAO report concluded that, due to widespread cybersecurity weaknesses at most federal

[23] U.S. Gov't Accountability Office, *DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System* (Jan. 2016) http://www.gao.gov/assets/680/674829.pdf (hereafter "GAO Cybersecurity Report").
[24] GAO Cybersecurity Report at 8.
[25] *Id*. at 7-8.
[26] *Id*. at 8.
[27] GAO Sensitive Data Protection Report.
[28] *Id*. at unpaginated "Highlights" section.
[29] *Id*.

agencies, "federal systems and information, as well as sensitive personal information about the public, will be at an increased risk of compromise from cyber-based attacks and other threats."[30]

Data breaches have directly impacted DHS information systems in recent years. For example, in 2014, a DHS contractor conducting background investigations for the agency experienced a data breach that compromised the records of at least 25,000 employees, including undercover investigators.[31] In 2015, another DHS contractor suffered a data breach that affected as many as 390,000 people associated with DHS, including current and former employees as well as contractors and job applicants.[32] More recently, a 16-year-old teenage boy was arrested in connection with hacks that exposed the information of more than 20,000 Federal Bureau of Investigation ("FBI") employees and 9,000 DHS employees, as well as the personal email accounts of DHS Secretary Jeh Johnson and Central Intelligence Agency ("CIA") director John Brennan.[33] Overall, the number of government data breaches, including for DHS, has exploded in the last decade, rising from 5,503 in 2006 to 67,168 in 2014.[34]

These weaknesses in DHS databases increase the risk that unauthorized individuals could read, copy, delete, add, or modify sensitive information contained in the FALCON Database. Accordingly, DHS should maintain only records that are relevant and necessary to ICE and CBP investigations. To the extent that DHS continues to collect this vast array of sensitive personal information, DHS should limit disclosure to only those agencies and government actors that

---

[30] *Id*. at 12.
[31] Jim Finkle & Mark Hosenball, *U.S. Undercover Investigators Among Those Exposed in Data Breach*, REUTERS (Aug. 22, 2014), http://www.reuters.com/article/us-usa-security-contractor-cyberattack-idUSKBN0GM1TZ20140822.
[32] Alicia A. Caldwell, *390,000 Homeland Employees May Have Had Data Breached*, ASSOCIATED PRESS (June 15, 2015), http://www.pbs.org/newshour/rundown/390000-homeland-employees-may-have-had-data-breached/.
[33] Alexandra Burlacu, *Teen Arrested Over DHS and FBI Data Hack*, TECH TIMES (Feb. 13, 2016), http://www.techtimes.com/articles/133501/20160213/teen-arrested-over-dhs-and-fbi-data-hack.htm.
[34] U.S. Gov't Accountability Office, *Federal Agencies Need to Better Protect Sensitive Data* 4 (Nov. 17, 2015), http://www.gao.gov/assets/680/673678.pdf [hereinafter "GAO Sensitive Data Protection Report"].

require the information as a necessity. Further, DHS should strictly limit the use of this information to the purpose for which it was originally collected.

There is also reason to be concerned about foreign governments compromising the FALCON Database. Foreign governments continue to show a willingness to interfere with and infiltrate government agencies.[35] The ability for foreign government to access and provide information for the Database is particularly concerning given recent revelations that foreign governments have been willing to provide false information that has the potential to derail investigations.[36] While foreign officials are only given access to trade data, allowing such access can potentially provide an entry point for a foreign agent to access all of the data contained in the Database.

b. FALCON Database Covers Broad Categories of Individuals and Implicates Individuals Who Are Not Under Investigation

The DHS proposes to collect the previously described personal data, including data for individuals who are not themselves under ICE investigation. The FALCON Database would contain records on ICE personnel or personnel from law enforcement agencies working with ICE; individuals who are associated with an ICE investigation, including victims, witnesses, and associates; individuals alleged to have been involved in illegal or suspicious activities; and individuals reporting suspicious or illegal activity.[37]

---

[35] Brian Ross & Pete Madden, *United States Remains Vulnerable to North Korean Cyber-Attack, Analysts Say,* ABC News, Apr. 22, 2017, http://abcnews.go.com/International/united-states-remains-vulnerable-north-korean-cyber-attack/story; David E. Sanger, *Putin Ordered 'Influence Campaign' Aimed at U.S. Election, Report Says,* New York Times, Jan. 6, 2017, https://www.nytimes.com/2017/01/06/us/politics/russia-hack-report.html.

[36] Karoun Demirjian & Devlin Barrett, *How a Dubious Russian Document Influenced the FBI's Handling of the Clinton Probe,* Washington Post, May 24, 2017, https://www.washingtonpost.com/world/national-security/how-a-dubious-russian-document-influenced-the-fbis-handling-of-the-clinton-probe/2017/05/24/f375c07c-3a95-11e7-9e48-c4f199710b69_story.html.

[37] FALCON SORN at 20,907.

By collecting, maintaining, and disclosing the records of such a broad variety of people, DHS could create detailed profiles of individuals who are not themselves the target of any investigation, do not work for the government, and who may be trying to aid ICE and CBP in carrying out their statutorily prescribed duties. Maintaining so much information and exempting it from Privacy Act protections will only serve to frustrate ICE and CBP operations as individuals may be unlikely to come forward with information about crimes or specific activity knowing that information may be kept about them personally. Furthermore, given ongoing concerns about data security, these individuals could effectively be placing themselves in significant danger if the database is breached and information about victims or witnesses who come forward are compromised.

III. Proposed Routine Uses Would Circumvent Privacy Act Safeguards and Contravene Legislative Intent

The Privacy Act's definition of "routine use" is precisely tailored, and has been narrowly prescribed in the Privacy Act's statutory language, legislative history, and relevant case law. The FALCON Database contains a potentially broad category of personally identifiable information. By disclosing information in a manner inconsistent with the purpose for which the information was originally gathered, the DHS exceeds its statutory authority to disclose personally identifiable information without obtaining individual consent.

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[38] Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by

[38] S. Rep. No. 93-1183 at 1 (1974).

Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[39]

The Privacy Act prohibits federal agencies from disclosing records they maintain "to any person, or to another agency" without the written request or consent of the "individual to whom the record pertains."[40] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[41] One of these exemptions is "routine use."[42] "Routine use" means "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."[43]

The Privacy Act's legislative history and a subsequent report on the Act indicate that the routine use for disclosing records must be specifically tailored for a defined purpose for which the records are collected. The legislative history states that:

> [t]he [routine use] definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information . . . or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[44]

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act— interpreted the above Congressional explanation of routine use to mean that a "'routine use' must be not only compatible with, but related to, the purpose for which the record is maintained."[45]

---

[39] Pub. L. No. 93-579 (1974).
[40] 5 U.S.C. § 552a(b).
[41] *Id*. §§ 552a(b)(1)–(12).
[42] *Id*. § 552a(b)(3).
[43] 5 U.S.C. § 552a(a)(7).
[44] *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[45] *Id*.

Subsequent Privacy Act case law limits routine use disclosures to a precisely defined system of records purpose. In *United States Postal Service v. National Association of Letter Carriers, AFL-CIO*, the Court of Appeals for the D.C. Circuit determined that "the term 'compatible' in the routine use definitions contained in [the Privacy Act] was added in order to limit interagency transfers of information."[46] The Court of Appeals went on to quote the Third Circuit and made clear, "[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."[47]

The FALCON SORN proposes numerous routine uses that are incompatible with the purpose for which the data was collected.[48] Proposed Routine Use H would permit the agency to disclose information contained in the FALCON Database:

> To Federal, State, local, tribal, territorial, foreign or international agencies, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual; the issuance, grant, renewal, suspension, or revocation of a security clearance, license, contract, grant, or other benefit; or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit.[49]

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

> To international, foreign, intergovernmental, and multinational government agencies, authorities, and organizations in accordance with law and formal or informal international arrangements.[50]

---

[46] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[47] *Id*. at 145 (quoting *Britt v. Natal Investigative Serv*., 886 F.2d 544, 549-50 (3d. Cir. 1989). *See also Doe v. U.S. Dept. of Justice*, 660 F.Supp.2d 31, 48 (D.D.C. 2009) (DOJ's disclosure of former AUSA's termination letter to Unemployment Commission was compatible with routine use because the routine use for collecting the personnel file was to disclose to income administrative agencies); *Alexander v. F.B.I*, 691 F. Supp.2d 182, 191 (D.D.C. 2010) (FBI's routine use disclosure of background reports was compatible with the law enforcement purpose for which the reports were collected).
[48] FALON SORN at 20,907.
[49] *Id.*
[50] *Id*.

Proposed Routine Use O would permit DHS to disclose information:

> To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, where there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy. [51]

The DHS proposes to disclose FALCON Database information for purposes that do not relate to ICE or CBP investigations. Determinations regarding employment or licensing as contemplated by Routine Use H is entirely unrelated to this purpose. This Routine Use 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."[52]

DHS also proposes to create a "Public Relations" exemption to the Privacy Act through Routine Use O that would permit the agency to release personal information to the media or members of the general public if there was a "legitimate public interest" unless the DHS determines that it is an "unwarranted invasion of personal privacy."[53] This Routine Use is unnecessarily broad especially given the number of people to be included in the proposed database and threatens to mistakenly expose the personal information of individuals. DHS should remove this 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 the DHS.

In addition, the proposed routine uses that would permit the DHS to disclose records, subject to the Privacy Act, to foreign, international, and private entities should be removed. The

---

[51] *Id*.
[52] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[53] FALCON SORN at 20,907.

Privacy Act only applies to records maintained by United States government agencies.[54] Releasing information to private and foreign entities does not protect individuals covered by this records system from Privacy Act violations.

IV. The DHS Proposes Broad Exemptions for the FALCON Database, Contravening the Intent of the Privacy Act of 1974

DHS proposes to exempt the Database from key Privacy Act obligations, such as the requirement that records be accurate and relevant, or that individuals be allowed to access and amend their personal records.

When Congress enacted the Privacy Act in 1974, it sought to restrict the amount of personal data that federal agencies were able to collect.[55] Congress further required agencies to be transparent in their information practices.[56] In *Doe v. Chao*,[57] 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."[58]

But despite the clear pronouncement from Congress and the Supreme Court on accuracy and transparency in government records, DHS proposes to exempt the Database from compliance with the following safeguards: 5 U.S.C. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8); and (g).[59] These provisions of the Privacy Act require agencies to:

---

[54] 5 U.S.C. § 552a(b).
[55] S. Rep. No. 93-1183, at 1 (1974).
[56] *Id*.
[57] *Doe v. Chao*, 540 U.S. 614 (2004).
[58] *Doe*, 540 U.S. at 618.
[59] 81 Fed. Reg. 9789, 9790.

- grant individuals access to an accounting of when, why, and to whom their records have been disclosed;[60]
- inform parties to whom records have been disclosed of any subsequent corrections to the disclosed records;[61]
- allow individuals to access and review records contained about them in the database and to correct any mistakes;[62]
- collect and retain only such 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";[63]
- collect information from the individual to the greatest extent possible, when such information would have an adverse effect on the individual;[64]
- inform individuals from whom they request information the purposes and routine uses of that information, and the effect of not providing the requested information;[65]
- notify the public when it establishes or revises a database, and provide information on the categories of information sources and procedures to access and amend records contained in the database;[66]
- ensure that all records used to make determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness;[67]
- serve notice to an individual whose record is made available under compulsory legal process; and[68]
- submit to civil remedies and criminal penalties for agency violations of the Privacy Act.[69]

Several of the DHS claimed exemptions would further exacerbate the impact of its overbroad categories of records and routine uses in this system of records. The DHS exempts itself from § 552a(e)(1), which requires agencies to maintain only those records relevant to the agency's statutory mission. The agency exempts itself from § 552a(e)(4)(I), which requires agencies to disclose the categories of sources of records in the system. And the agency exempts itself from its Privacy Act duties under § 552a(e)(4)(G) and (H), which allows individuals to access and correct information in its records system. In other words, the DHS claims the

[60] 5 U.S.C. § 552a(c)(3).
[61] *Id.* § 552a(c)(4).
[62] *Id*. § 552a(d).
[63] *Id*. § 552a(e)(1).
[64] *Id*. § 552a(e)(2).
[65] *Id*. § 552a(e)(3).
[66] *Id*. § 552a(e)(4)(G), (H), (I).
[67] *Id*. § 552a(e)(5).
[68] *Id.* § 552a(e)(8).
[69] *Id.* § 552a(g).

authority to collect any information it wants without disclosing where it came from or even acknowledging its existence. The net result of these exemptions, coupled with the DHS's proposal to collect and retain virtually unlimited information unrelated to any purpose Congress delegated to the agency, would be to diminish the accountability of the agency's information collection activities.

The DHS also proposes exemption from maintaining records with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[70] In other words, the DHS admits that it contemplates collecting information that will not be relevant or necessary to a specific investigation. The agency claims that the inability to determine, in advance, whether information is accurate, relevant, timely, and complete precludes its agents from complying with the obligation to ensure that the information meets these criteria after it is stored.[71] By implication, the agency objects to guaranteeing "fairness" to individuals in the FALCON Database.

It is inconceivable that the drafters of the Privacy Act would have permitted a federal agency to maintain a database on U.S. citizens containing so much personal information and simultaneously be granted broad exemptions from Privacy Act obligations. It is as if the agency has placed itself beyond the reach of the American legal system on the issue of greatest concerns to the American public – the protection of personal privacy. Consistent and broad application of Privacy Act obligations are the best means of ensuring accuracy and reliability of database records, and the DHS must reign in the exemptions it claims for its FALCON Database.

[70] 5 U.S.C. § 552a(e)(5).
[71] FALCON PIA at 20,846.

V. Conclusion

For the foregoing reasons, the FALCON Database is contrary to the core purpose of the federal Privacy Act. Accordingly, the DHS must limit the records contained in the Database and the individuals to whom the records pertain, narrow the scope of its proposed Privacy Act exemptions, and remove the proposed unlawful routine use disclosures from the FALCON system of records.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Jeramie D. Scott
Jeramie D. Scott
EPIC National Security Counsel

/s/ Kim Miller
Kim Miller
EPIC Policy Fellow

/s/ Ellen Coogan
Ellen Coogan
IPIOP Law Clerk