COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

Joined By

THE ALA WASHINGTON OFFICE
THE BILL OF RIGHTS DEFENSE COMMITTEE
THE CENTER FOR FINANCIAL PRIVACY AND HUMAN RIGHTS
THE CENTER FOR MEDIA AND DEMOCRACY
CONSUMER ACTION
CONSUMER FEDERATION OF AMERICA
THE CYBER PRIVACY PROJECT
ELECTRONIC FRONTIER FOUNDATION
THE LIBERTY COALITION
OMB WATCH
OPENTHEGOVERNMENT.ORG
PATIENT PRIVACY RIGHTS
PRIVACY ACTIVISM
THE PRIVACY JOURNAL
PRIVACY RIGHTS CLEARINGHOUSE
PRIVACY RIGHTS NOW COALITION
WORLD PRIVACY FORUM

to

THE DEPARTMENT OF HOMELAND SECURITY

"Notice of Proposed Rulemaking"

DHS-2011-0060

and

"Notice of Privacy Act System of Records"

DHS-2011-0061

August 5, 2011

By a Notice of Proposed Rulemaking ("NPRM") and a System of Records Notice ("SORN"),[1] both published in the Federal Register on July 6, 2011, the Department of Homeland Security ("DHS") proposed to introduce a new system of records containing names, dates of birth, places of birth, biometrics and photographic data, passport information, driver's license information, and "other available identifying particulars."[2] The agency will maintain unique identifiers for each data subject in the new system.[3]

The agency proposes to exempt the proposed system from the following legal rights and obligations that Congress created under the Privacy Act:

- The obligation to maintain all government records pertaining to an individual with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual" 5 U.S.C. § 552a(e)(5).

- The obligation only to maintain records about individuals when "relevant and necessary" for a government agency to accomplish an authorized purpose. 5 U.S.C. § 552a(e)(1).

- The obligation to publish the agency procedures for individuals to determine if there are government records pertaining to them, and to access and contest the content of those records. 5 U.S.C. §§ 552a(e)(4)(G)-(H); 5 U.S.C. § 552a(f).

- The obligation to submit to civil remedies and criminal penalties for agency violations of the Privacy Act. 5 U.S.C. § 552a(g)(1), (i), (j).

- The right for individuals to request and gain access to government records about the individuals, and to review the records and have copies made. 5 U.S.C. § 552a(d)(4).

- The right for subjects of government records to request an "accurate accounting of – the date, nature, and purpose of each disclosure" of those records. 5 U.S.C. § 552a(c)(3).

---

[1] Notice of Privacy Act System of Records, Privacy Act of 1974; Department of Homeland Security/All-030 Use of the Terrorist Screening Database System of Records, 76 Fed. Reg. 39408 (July 6, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-07-06/pdf/2011-16807.pdf [hereinafter "System of Records Notice"]; Notice of Public Rulemaking, Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ALL-030 Use of the Terrorist Screening Database System of Records, 76 Fed. Reg. 39,315, 39,317 (Jul. 6 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-07-06/pdf/2011-16806.pdf; [hereinafter "Notice of Public Rulemaking"].

[2] Dept. of Homeland Security, Privacy Impact Assessment for the Watchlist Service, 4, July 14, 2010, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_wls.pdf. [hereinafter "Privacy Impact Assessment"].

[3] *Id*.

- The right to request an "accurate accounting" of the name and addresses of the agencies or people to whom such records are disclosed. 5 U.S.C. § 552a(c)(3).

- The obligation to inform each individual whom the agency asks to supply information about the legal authority and principal purposes for the collection. 5 U.S.C. § 552a(e)(3).

- The right to notify government agencies and personnel about corrections to government records pertaining to the individuals. 5 U.S.C. § 552a(c)(4).

- The right to request amendments to such government records that the individual believes are not accurate, relevant, timely or complete; and also to a prompt government response either complying with the request or providing the individual reasons for the government's refusal to comply. 5 U.S.C. § 552a(e)(5).[4]

The DHS has stated that it "does not control the accuracy of the information" within this system of records, leaving the responsibility for correcting errors to the Department of Justice and the Federal Bureau of Investigation.[5] The agency has also stated that "individuals do not have an opportunity to decline to provide information."[6]

Pursuant to the DHS notices in the Federal Register, the Electronic Privacy Information Center ("EPIC") and undersigned privacy, consumer rights, and civil rights organizations hereby submit these comments and recommendations to address the substantial privacy risks posed by the proposal. DHS should suspend the proposal pending a full review of the privacy, security, and legal implications of the program, including compliance with the federal Privacy Act. If the agency proceeds with the WLS program, the system must, at a minimum: (1) adhere to Congress's intent to maintain transparent and secure government recordkeeping systems; (2) provide individuals judicially enforceable rights of notice, access, and correction; (3) conform to a revised SORN and NPRM that includes requirements for the agency to respect individuals'

[4] Notice of Public Rulemaking, *supra* note 1, at 39317.
[5] Privacy Impact Assessment, *supra* note 2, at 3, 6.
[6] *Id*. at 14.

rights to control their information in possession of federal agencies, as the Privacy Act requires; and (4) premise its technological and security approach on decentralization.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has particular interest in preserving privacy safeguards established by Congress, in the development of new information systems operated by the federal government.[7]

The American Library Association ("ALA") Washington Office is dedicated to the public's right to a free and open information society. Intellectual freedom is a basic right in a democratic society and a core value of the library profession. As the oldest and largest library association in the world, ALA reflects the library community's long-standing commitment to First Amendment and personal privacy, and actively defends the right of library users to read, seek information, and speak freely as guaranteed by the First Amendment. In keeping with these principles, the ALA promotes the confidentiality of library users and argues that the collection of personally identifiable information, regardless of the technology used, brings with it a legal and

[7] *See*, *e.g.*, Electronic Privacy Information Center: Passenger Profiling, http://epic.org/privacy/airtravel/profiling.html; Electronic Privacy Information Center: Department of Homeland Security Chief Privacy Office and Privacy, http://epic.org/privacy/dhs-cpo.html; Electronic Privacy Information Center, Secure Flight, http://epic.org/privacy/airtravel/secureflight.html; Electronic Privacy Information Center: EPIC Alert 16.09, "Report Finds Failure and Delay in Watchlist Name Removal," (May 15, 2009), *available at* http://epic.org/alert/EPIC_Alert_16.09.html; Statement of Lillie Coney, Associate Director, Electronic Privacy Information Center to House Committee on Homeland Security, Subcommittee on Transportation Security and Infrastructure Protection (Sept. 9, 2008), *available at* http://epic.org/privacy/airtravel/watchlist_test_090908.pdf; Electronic Privacy Information Center, 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; Comments of the Electronic Privacy Information Center, AAG/A Order No. 006-2005: Terrorist Screening Records System (Sept. 6, 2005); Statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center to National Commission on Terrorist Attacks Upon the United States (Dec. 8, 2003), *available at* http://epic.org/privacy/terrorism/911commtest.pdf.

ethical obligation to protect confidentiality as part of the public's "right to read." ALA is a nonprofit organization of over 65,000 librarians, library trustees, and other friends of libraries.

The Bill of Rights Defense Committee ("BORDC") is a national non-profit grassroots organization. BORDC defends the rule of law and rights and liberties challenged by overbroad national security and counter-terrorism policies. BORDC supports an ideologically, ethnically, geographically, and generationally diverse grassroots movement to protect and restore these principles by encouraging widespread civic participation; educating people about the significance of our rights; and cultivating grassroots networks to convert concern, outrage, and fear into debate and action.

The Center for Financial Privacy and Human Rights ("CFPHR") was founded in 2005 to defend privacy, civil liberties and market economics. The Center is a non-profit human rights and civil liberties organization whose core mission recognizes traditional economic rights as a necessary foundation for a broad understanding of human rights. CFPHR is part of the Liberty and Privacy Network, a non-governmental advocacy and research 501(c)(3) organization.

The Center for Media and Democracy is an independent, non-profit, non-partisan, public interest organization that focuses on investigating and countering spin by corporations, industry and government; informing and assisting grassroots action that promotes public health, economic justice, ecological sustainability, human rights, and democratic values; advancing transparency and media literacy to help people recognize the forces shaping the information they receive about important issues affecting their lives; and promoting "open content" media that enable people from all walks of life to "be the media" and help write the history of these times.

Consumer Action is a nonprofit organization that has championed the rights of underrepresented consumers nationwide since 1971. Throughout its history, the organization has

dedicated its resources to promoting financial literacy and advocating for consumer rights in both the media and before lawmakers to promote economic justice for all. With the resources and infrastructure to reach millions of consumers, Consumer Action is one of the most recognized, effective, and trusted consumer organizations in the nation.

The Consumer Federation of America ("CFA") is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. Today, nearly 300 of these groups participate in the federation and govern it through their representatives on the organization's Board of Directors. CFA is a research, advocacy, education, and service organization. As a research organization, CFA investigates consumer issues, behavior, and attitudes through surveys, focus groups, investigative reports, economic analysis, and policy analysis. As an advocacy organization, CFA works to advance pro-consumer policies on a variety of issues before Congress, the White House, federal and state regulatory agencies, state legislatures, and the courts. As an education organization, CFA disseminates information on consumer issues to the public and news media, as well as to policymakers and other public interest advocates. As a service organization, CFA assists individuals and organizations.

The Cyber Privacy Project ("CPP") addresses issues about privacy raised in today's networked world. In upholding the belief that privacy is essential to democratic society, the Cyber Privacy Project anchors its approach in realizing the beneficial potential of the Constitution, laws, and policies of the United States. CPP calls for implementation of privacy protections based on First Amendment rights of privacy and anonymity, Fourth Amendment rights against unreasonable searches and seizures, the Fifth and Fourteenth Amendment rights to due process and protection of liberty, and Ninth Amendment un-enumerated rights to privacy. It

also calls upon similar principles in international human rights documents, state constitutions, and codes of ethics. CPP gathers momentum behind its policy recommendations by serving as a source for the media and public discussions. CPP makes its issues relevant to the majority of citizens by using and addressing new forms of technological communication in order to convey its message to a wide audience of individuals and groups.

The Electronic Frontier Foundation ("EFF") is a nonprofit, member-supported civil liberties organization working to protect rights in the information society. EFF actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become more prevalent in society.

The Liberty Coalition works to help organize, support, and coordinate transpartisan public policy activities related to civil liberties and basic rights. We work in conjunction with groups of partner organizations that are interested in preserving the Bill of Rights, personal autonomy and individual privacy.

OMB Watch is a nonprofit research and advocacy organization in Washington, D.C., established in 1983 to promote open government, accountability, and citizen participation. OMB Watch has particular interest in ensuring that federal information policy supports transparent and accountable government.

OpenTheGovernment.org is a coalition of consumer, good government and limited-government groups, environmentalists, journalists, library groups, labor and others united to make the federal government a more open place in order to make us safer, strengthen public trust in government, and support our democratic principles.

Patient Privacy Rights ("PPR") is the nation's leading health privacy watchdog and consumer voice for building ethical, trustworthy health IT systems. Patients won't see or trust

physicians unless they control who sees and uses sensitive personal health information. PPR educates the public and holds industry and government accountable. Today PPR has over 12,000 members in all 50 states and represents 10.3 million Americans through the bipartisan Coalition for Patient Privacy. PPR champions the right to health information privacy and privacy-enhancing technologies (privacy-by-design) so patients can move the right personal information to the right person at the right time -- and prevent the sale, misuse, surveillance, and onward disclosures of protected health information without consent by industry, research, and government. Recently PPR and the University of Texas LBJ School of Public Affairs co-sponsored the first-ever international Summit on the Future of Health Privacy.

Privacy Activism is a consumer privacy organization focusing primarily on online consumer privacy issues, raising public understanding of complex questions about privacy, and helping people make informed choices.

Privacy Journal is the most authoritative and long standing publication in the world on the individual's right to privacy. This acclaimed monthly newsletter covers current events in new technology and its impact on privacy, useful tips for protecting individual privacy, and the latest updates on court decisions, legislation, professional conferences, and corporate practices. Publisher Robert Ellis Smith is recognized as a leading expert on the right to privacy in the U.S. He is an experienced journalist, a lawyer, and an author of several essential books on privacy.

The Privacy Rights Clearinghouse ("The PRC") is a nonprofit consumer education and advocacy organization, established in 1992 and based in San Diego, CA. The PRC advises individuals on a variety of informational privacy issues, and has published more than 50 Fact Sheets providing practical information individuals may employ to safeguard their personal

information. The PRC has submitted comments for numerous federal and state administrative proceedings.

Privacy Rights Now was organized by Ralph Nader and Remar Sutton to highlight the efforts of the key non-profit organizations that care about the value of our private lives.

The World Privacy Forum is a nonprofit, non-partisan 501(c)(3) public interest research group. The organization is focused on conducting in-depth research, analysis, and consumer education in the area of privacy. It is the only privacy-focused public interest research group conducting independent, longitudinal work. The World Privacy Forum has had notable successes with its research, which has been groundbreaking and consistently ahead of trends. World Privacy Forum reports have documented important new areas, including medical identity theft. Areas of focus for the World Privacy Forum include health care, technology, and the financial sector. The Forum was founded in 2003 and works both nationally and internationally.

I. The Watchlist Service Will Centralize and Expand The Agency's Collection and Disclosure of Sensitive Personal Information

The Federal Bureau of Investigation ("FBI") and the Department of Justice ("DOJ") operate the Terrorist Screen Center ("TSC").[8] The TSC maintains the "Terrorist Screening Database" ("TSDB"), a database filled with the sensitive personal information of an undisclosed set of individuals.[9] DHS receives TSDB data, using personal information to determine whether an individual "meets the criteria for a particular immigration or naturalization benefits" (sic), and to facilitate its own counterterrorism, law enforcement, and border security operations.[10]

[8] Privacy Impact Assessment, *supra* note 2, at 2
[9] *Id*.
[10] *Id*. at 2, 7.

DHS has now proposed the Watchlist Service ("WLS") as a mechanism to centralize the interagency transfer of data from TSC's TSDB to DHS. DHS intends WLS to serve as a singular "main repository." DHS contemplates intra-agency transfers of WLS data "downstream" into four different DHS systems of records:

1) Transportation Security Threat Assessment System (managed by the TSA Office of Transportation Threat Assessment and Credentialing)
2) Secure Flight Records (managed by the TSA)
3) TECS (managed by the CBP Passenger Systems Program Office)
4) IDENT (managed by the US-VISIT Program)[11]

Each system of records is separately managed by a component of the Department of Homeland Security. There will also be upstream disclosure, as each component records encounters with a potential terrorist match and transmits that information to the FBI, the DOJ, and DHS.[12] The WLS includes a "mirror" of the TSDB.[13] A "mirror" is a near real-time copy that synchronizes itself with the original database by adding, modifying, or deleting data in accord with updates to records in the original.[14] DHS's proposal calls for the DHS Screening Coordination Office to manage screening and facilitate the abovementioned "downstream" information disclosure.[15] The DHS Customs and Border Patrol will serve as the "technical steward" that implements the automated Watchlist feed.[16]

[11] *Id. at* 2-3.
[12] *Id.* at 3.
[13] *Id*. at 8.
[14] *Id.* at 9.
[15] *Id*. at 3.
[16] *Id*. at 3.

II. The Privacy Act Requires DHS To Afford Fundamental Privacy Rights to the Subjects of WLS Records

When it enacted the Privacy Act, 5 U.S.C. § 552a, in 1974, Congress sought to restrict the amount of personal information federal agencies could collect, and it required agencies to be transparent in their information practices.[17] Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies." Congress also emphasized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[18] 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:

> [I]n 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." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[19]

Despite these clear statements of legislative mandate, DHS is proposing to circumvent a number of meaningful privacy protections Congress established in the Privacy Act.[20] DHS also claims an exemption from paying any civil remedies for violating any of the Act's provisions that the agency claims do no apply.[21]

---

[17] S. Rep. No. 93-1183 at 1 (1974).
[18] Pub. L. No. 93-579 (1974).
[19] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[20] *See* Notice of Public Rulemaking, *supra* note 1, at 39317.
[21] *See* id.

A. DHS Seeks to Exempt the WLS from Privacy Act Accounting Requirements

DHS seeks "routine use" exemptions from the agency's Privacy Act obligations regarding its disclosures of individuals' personal information.[22] Congress has ordered all executive agencies to disclose, upon any data subject's request, an accurate accounting of "the date, nature, and purpose of each disclosure of a record [regarding that data subject] to any person or to another agency."[23] Congress has also mandated that agencies "inform any person or other agency about any correction or notation of dispute made by the agency [about the accuracy of a data subject's records]."[24] DHS seeks to circumvent these requirements, arguing that compliance could "reveal investigative interest" on the part of DHS.[25] The agency alleges that such a revelation would "present a serious impediment to law enforcement efforts and/or efforts to preserve national security."[26] But DHS proffers no evidence for this claim.

Vague national security and law enforcement concerns vindicate neither the government's secretive collection of personal information nor subsequent disclosures through WLS between agencies and government personnel. Without specific justifications linked to the WLS program, the agency is not authorized to evade the meaningful safeguards Congress designed to ensure accuracy and legality of government recordkeeping. The Senate Report from 1974 emphasizes that "it is fundamental to the implementation of any privacy legislation that no system of personal information be operated or maintained in secret by a Federal agency."[27] In those few instances in which a limited exemption for national security and law enforcement may be recognized, the same report specifies that exemptions are "not intended to provide a blanket

---

[22] *Id*. at 39317.
[23] *Id.* at 39317. See 5 U.S.C. §§ 552a(c)(1)(A)-(B), (c)(3).
[24] Notice of Public Rulemaking, *supra* note 1, at 39317. *See* 5 U.S.C. 552a(c)(4).
[25] Notice of Public Rulemaking, *supra* note 1, at 39317.
[26] *Id.* See 5 U.S.C. §§ 552a(c)(3), (c)(4).
[27] S. Rep. No. 93-1183, at 74 (1974).

exemption to all information systems or files maintained by an agency which deal with national defense and foreign policy information."[28]

In light of Congress's intent to achieve meaningful government transparency in recordkeeping practices, DHS should retract its claimed exemptions and reassess the agency's overly broad justification for failing to comply with its Privacy Act obligations.

B. DHS Seeks to Prevent Individuals from Accessing and Correcting Erroneous Records in the WLS

In the same notice, DHS also seeks to exempt the WLS from Privacy Act provisions guaranteeing citizens the right to access and correct records containing information about them.[29] The Privacy Act provides, among other things, that an individual must have notice of records an agency maintains about him or her, including the purpose, authority, and routine uses for that information.[30] The Act guarantees meaningful access to those records; and also that the agency must publish a notice of the existence of records in the Federal Register, along with the procedures individuals can use to obtain access and correct them.[31] The agency has claimed "routine use" exemptions from these requirements, citing hypothetical risks, including witness tampering, heightened efforts to avoid detection, and exposure of confidential informants.[32] The agency also maintains that the Privacy Act's requirement that the government correct inaccuracies in its records presents an "unreasonable administrative burden."[33]

The legislative history of the Privacy Act demonstrates that rights of notice, access, and correction were central to what Congress sought to achieve: "The committee believes that this

---

[28] *Id*. at 74.
[29] Notice of Public Rulemaking, *supra* note 1, at 39317.
[30] 5 U.S.C. § 552a(e)(3).
[31] 5 U.S.C. §§ 552a(d), (e)(4)(G)-(I), (f).
[32] Notice of Public Rulemaking, *supra* note 1, at 39317. *See* 5 U.S.C. §§ 552a(d), (e)(3), (e)(4)(G)-(I), (f).
[33] Notice of Public Rulemaking, *supra* note 1, at 39317. *See* 5 U.S.C. § 552a(d).

provision is essential to achieve an important objective of the legislation: ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records."[34] Even where information is withheld during a period of specific investigation, data subjects are legally entitled to notice, after an investigation is completed or made public, about the information stored about them in all government systems of records. The notion of an investigation that is ongoing in perpetuity and without completion would be absurd. Moreover, the use of confidential informants raises the possibility that investigations might be premised on malicious misinformation spread by bad actors. Individuals deserve the right Congress granted them to correct misinformation in government records, administrative burden notwithstanding. Rather than claiming blanket exemptions, the DHS could promulgate rules that would require notification only after an active investigation had been concluded, or with sensitive information, such as the identity of confidential informants, redacted prior to release.

Given the centrality of individual rights to notice, access, and correction, DHS should withdraw its proposed exemptions and narrow the grounds on which it purports to avoid its obligations under the Privacy Act.

C. DHS Seeks Authority to Collect Irrelevant, Unnecessary, and Otherwise Inaccurate Information

Congress prescribed record keeping standards for agencies in order to ensure quality control and protect privacy. The Privacy Act explicitly limits agencies to "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency" as laid out in Congressional authorizations.[35] For information that agencies do collect, agencies must

[34] H.R. Rep. No. 93-1416, at 15 (1974).
[35] 5 U.S.C. § 552a(e)(1).

maintain any records that inform official decisions about individual data subjects with "such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination."[36] DHS claims "routine use" exemptions from both of these requirements. In doing so, the agency admits that it contemplates collecting information that will not be relevant or necessary to a specific investigation.[37] The agency's alleged purpose in consciously flouting this requirement is to establish "patterns of unlawful activity."[38] The agency also 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.[39] By implication, the agency objects to guaranteeing "fairness" to individuals on the Watchlist.[40]

The sweeping exemption DHS has proposed would enable the agency to collect and maintain information unrelated to any purpose Congress delegated to the agency. Secretive government lists without any meaningful safeguards present a very real risk of "mission creep," in which a system is pressed into unintended or unauthorized uses. Under this proposal, the agency would have the right to maintain and rely upon information it does not know to be accurate, relevant, timely, or complete without recourse – the right to subject citizens to arbitrary decisions. This is exactly what Congress sought to remedy with the Privacy Act.

The Privacy Act's "relevant and necessary" requirement is a fundamental part of the law's protections, as it is "[d]esigned to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course

---

[36] 5 U.S.C. § 552a(e)(5).
[37] Notice of Public Rulemaking, *supra* note 1, at 39317. *See* 5 U.S.C. § 552a(e)(1).
[38] *Id*.
[39] Notice of Public Rulemaking, *supra* note 1, at 39317. *See* 5 U.S.C. § 552a(e)(5).
[40] *See* 5 U.S.C. § 552a(e)(5).

of meeting government's needs, its action may not be arbitrary."[41] Presumably, facts in the system helpful to the DHS in a particular investigation would be relevant and necessary to that investigation, and thus in compliance with the Privacy Act. Even if DHS decided to accommodate exceptions to this general truism, the agency could promulgate a rule limiting its exemptions to "patterns of unlawful activity" and/or "appropriately marked field reports from DHS agents."

Considering the common sense benefits of collecting and relying upon high quality information, DHS should void these claimed exemptions and instead affirm the agency's commitment to maintaining relevant and necessary records with accurate, timely, and complete information.

III. The Watchlist Program Subjects Individuals To Inherent Privacy Risks

In the Department's Privacy Impact Assessment, the agency has highlighted privacy flaws that centralizing WLS data will purportedly solve.[42] Tellingly, DHS has previously failed to publicize or fix these issues since the onset of its component parts. Rather than amending privacy flaws in the component systems, for the sake of complying with the legal obligations and securing sensitive data, the agency now raises them only to justify creating an even more privacy-defective System of Records.

For instance, in response to a question about the privacy risks of the existing system, the Department now admits that its current "lack of automation presents the risk for unintentional errors to be introduced in the processing of data, and increases the risk that the TSDB data used

[41] S. Rep. No. 93-3418 at 47 (1974).
[42] Privacy Impact Assessment, *supra* note 2.

by DHS is not synchronized with the authoritative source, the TSDB."[43] The Department now highlights this risk as a flaw.[44] However, previous Privacy Impact Assessments of WLS derivative components, including the agency's October 21, 2008 Privacy Impact Assessment regarding DHS's Secure Flight Program, failed to identify the lack of automation as a privacy risk when given the opportunity to do so.[45] The agency did make mention of the characteristic:

> Depending on the urgency, information may be transmitted electronically, in person, in paper format, via facsimile, or by telephone, as required by the circumstances necessitating such sharing. In most cases, the data will be transmitted between Secure Flight and other systems on the secured DHS information technology (IT) network.[46]

What is missing is any effort to identify the use of paper or fax or telephone as susceptible to "human error" in response to the direct prompt: "[g]iven the internal sharing, discuss what privacy risks were identified and how they were mitigated."[47] It is apparent the agency does not identify all material privacy risks in its Privacy Impact Assessments.

The current Assessment for the WLS fails subject to this same insufficient approach. The very process of centralization will introduce an entirely new tier of privacy risks, which the agency has failed to identify. The WLS Proposal will concentrate all interagency transfer of personal data in WLS records into a singular "main repository." The sensitive information in these records will include names, dates of birth, places of birth, biometrics and photographic data, passport information, driver's license information, and "other available identifying

[43] *Id.* at 7.
[44] *Id*. at 7.
[45] Dept. of Homeland Security, Privacy Impact Assessment for Secure Flight, July 14, 2010, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_wls.pdf.
[46] *Id*. at 15.
[47] *Id*. at 16.

particulars."[48] In addition, four different DHS offices will create, store, and transfer records of encounters with any listed individuals into the same system. The agency will also maintain a near real-time copy that synchronizes itself with the original database by adding, modifying, or deleting data in accord with updates to records in the original. What the agency is proposing will provide an appealing mark for thieves trying to create false identities for criminal activities. Further, a data breach involving this rich compendium of personal data would be a disaster for the agency and place the data subjects at risk for a variety of harms. DHS should seriously consider alternative approaches, as privacy is much better safeguarded by storing data in multiple, decentralized locations, and only when necessary.

As a result of this major oversight, due to an insufficient approach toward self-assessments, DHS should reconsider its approach to storing and transferring personal data and comply with the Privacy Act's safeguards to protect privacy and security.

IV. Conclusion and Final Recommendations

For the foregoing reasons, EPIC and the undersigned privacy, consumer rights, and civil rights organizations recommend that DHS suspend the WLS system pending a full review of the privacy and security implications of the program. The agency must revise its proposed system of records and fully assess its compliance with the federal Privacy Act. If the agency proceeds with the WLS program, the system must, at a minimum: (1) adhere to Congress's intent to maintain transparent and secure government recordkeeping systems; (2) provide individuals judicially enforceable rights of notice, access, and correction; (3) conform to a revised SORN and NPRM that includes requirements for the agency to respect individuals' rights to control their

[48] Dept. of Homeland Security, Privacy Impact Assessment for the Watchlist Service, 4, July 14, 2010, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_wls.pdf. [hereinafter "Privacy Impact Assessment"].

information in possession of federal agencies, as the Privacy Act requires; and (4) premise its technological and security approach on decentralization.

We anticipate the agency's specific and substantive responses to each of these proposals. The current NPRM is contrary to law, exceeds the scope of the agency's rulemaking authority, and should be withdrawn.

Sincerely,

Marc Rotenberg
EPIC Executive Director

Lillie Coney
EPIC Associate Director

John Verdi
EPIC Senior Counsel

Conor Kennedy
EPIC Appellate Advocacy Fellow