COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE DEPARTMENT OF HOMELAND SECURITY

"Systems of Records Notice"

DHS-2011-0003

March 3, 2011

By notice published on February 1, 2011, the Department of Homeland Security ("DHS") Office of Operations Coordination and Planning ("OPS") National Operations Center ("NOC"), has proposed to establish a new system of records. The "Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records"[1] will gather information from "online forums, blogs, public websites, and message boards," store and analyze the information gathered, and then "disseminate relevant and appropriate de-identified information to federal, state, local, and foreign governments and private sector partners."[2]

Pursuant to the DHS notice in the Federal Register, the Electronic Privacy Information Center ("EPIC") submits these comments and recommendations to address the substantial privacy risks raised by the DHS proposal.

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 constitutional values and the rule of law. EPIC has a particular interest in preserving privacy

---

[1] Privacy Act of 1974; Department of Homeland Security Office Operations Coordination and Planning–004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records, 76 Fed. Reg. 5603 (Feb. 1, 2011) [hereinafter *Systems of Records Notice*].
[2] *Id*. at 5603.

safeguards established by Congress and ensuring that new information systems developed and operated by the federal government comply with all applicable laws.[3]

Comments and Recommendations

EPIC submits the following comments and recommendations:

1. *DHS's Proposal Contravenes the Purpose and Intent of the Federal Privacy Act*

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal data that federal agencies could collect and to require government agencies to limit the collection, sharing, and use of individuals' personal information.[4] In 2004, the Supreme Court underscored the importance of Privacy Act restrictions upon agency use of personal data to protect privacy interests, noting that:

---

[3] *See, e.g.,* EPIC: Information Fusion Centers and Privacy, http://epic.org/privacy/fusion/; EPIC: EPIC v. Virginia Department of State Police: Fusion Center Secrecy Bill, http://epic.org/privacy/virginia_fusion/; Statement of Lillie Coney, EPIC Associate Director, to the Department of Homeland Security Data Privacy and Integrity Advisory Committee (Sept. 19, 2007), *available at* http://www.epic.org/privacy/fusion/fusion-dhs.pdf; Letter from Marc Rotenberg, EPIC Executive Director, and John Verdi, EPIC Staff Counsel, to Senate Committee on Homeland Security and Governmental Affairs and the Senate Subcommittee on State, Local, and Private Sector Preparedness and Integration (Apr. 17, 2008), *available at* http://www.epic.org/privacy/fusion/EPIC_ltr_Sen_Fusion_Ctrs.pdf; Press Release, EPIC, EPIC Obtains Documents Revealing Federal Role in State Fusion Center Secrecy (Apr. 11, 2008), *available at* http://epic.org/press/041108.html; Freedom of Information Act Request from John Verdi, Director, EPIC Open Government Project to Virginia State Police (Feb. 12, 2008), *available at* http://www.epic.org/privacy/fusion/VA_FOIA021208.pdf; Complaint, EPIC v. Martin and the Virginia Department of State Police (D. Va. 2007), *available at* http://www.epic.org/privacy/fusion/VA_FOIA_lawsuit_032108.pdf; EPIC: Open Government, http://epic.org/open_gov/; EPIC: Spotlight on Surveillance: "National Network" of Fusion Centers Raises Specter of COINTELPRO, http://epic.org/privacy/surveillance/spotlight/0607/; EPIC: Privacy, http://epic.org/privacy/; Statement of Lillie Coney, EPIC Associate Director, to ABA Conference, Computing and the Law: From Steps to Strides into the New Age (June 25-26, 2007), *available at* http://www.epic.org/epic/staff/coney/surveillance.pdf; Letter from EPIC, et. al to Rep. Bennie G. Thompson, Chair, U.S. House of Representatives Committee on Homeland Security, and Representative Peter T. King, Ranking Member, U.S. House of Representatives Committee on Homeland Security (Oct. 23, 2009), *available at* http://www.epic.org/security/DHS_CPO_Priv_Coal_Letter.pdf; EPIC: EPIC Alert 15.10, "EPIC Prevails in Virginia Fusion Center FOIA Case," (May 16, 2008), http://mailinglists.epic.org/pipermail/epic_news/2008-May/000001.html; EPIC: EPIC Alert 14.19, "DHS Privacy Advisory Panel Holds Hearing on Fusion Center," (Sept. 20, 2007), http://epic.org/alert/EPIC_Alert_14.19.html; EPIC: "DHS Releases Fusion Center Privacy Impact Assessment," EPIC Alert 15.25 (Dec. 23, 2008), http://mailinglists.epic.org/pipermail/epic_news/2008-December/000017.html; EPIC: "Documents Reveal Federal Role In Fusion Center Secrecy," EPIC Alert 15.08 (Apr. 17, 2008), http://epic.org/alert/EPIC_Alert_15.08.html; EPIC: Department of Homeland Security Chief Privacy Office and Privacy, http://epic.org/privacy/dhs-cpo.html.

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

> [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.[5]

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[6] The statute is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[7] The law thus seeks to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[8]

Contrary to the text and purpose of the Privacy Act, the proposed initiative targets search terms likely to retrieve embarrassing information, which the agency then intends to store for up to five years and package for dissemination through transnational and international networks.[9] The Privacy Act requires agencies to

> establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could

---

[5] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[6] S. Rep. No. 93-1183 at 1.
[7] Pub. L. No. 93-579 (1974).
[8] *Id*.
[9] Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 7, Jan. 6, 2011, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocialmedia_update.pdf

> result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.[10]

DHS's proposed initiative would enable the agency to "establish usernames and passwords," form social media profiles that will follow other accounts, deploy search tools, and record the results of an array of potentially sensitive search terms (stated examples of search terms include "illegal immigrants," "drill," "infection," "strain," "outbreak," "virus," "recovery," "deaths," "collapse," "human to animal," and "trojan.").[11]

The Privacy Act imposes limitations on the dissemination of personal information collected by an agency. In contravention of the text and purpose of the Act, DHS plans to regularly relay the records to "federal, state, local, tribal, territorial, foreign, or international government partners."[12] The DHS Chief Privacy Officer (CPO) has stated that the records would be shared both by "email and telephone" to contacts inside and outside of the agency.[13] The CPO further stated that "[n]o procedures are in place" to determine which users may access this system of records.[14] Even Department contractors will have full access to the system.[15] Moreover, the Secretary of the Department has an

---

[10] 5 U.S.C. § 552a(e)(10) (2010).

[11] System of Records Notice at 5603; Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 17-21, June 22, 2010, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_publiclyavailablesocial.media.pdf.

[12] System of Records Notice at 5604.

[13] Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 8, Jan. 6, 2011.

[14] Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 10, June 22, 2010x.

[15] *Id*.

affirmative statutory obligation to ensure that the agency "produces and disseminates unclassified reports and analytic products" based upon the information collects.[16]

DHS's proposed initiative also fails to satisfy Privacy Act requirements by failing to ensure the accuracy of records before disseminating them to state, local, tribal, and foreign governments, as well as private sector entities.[17] The Privacy Act requires agencies to make "reasonable efforts to assure that . . . records are accurate, complete, timely, and relevant for agency purposes" prior to their dissemination outside of the federal government.[18] DHS's proposed Social Media Monitoring Initiative, however, explicitly relies on unverified sources of information to construct records it intends to disseminate to state, local, tribal, territorial, foreign, and international governments. As the DHS CPO has stated, "[u]sers may accidentally or purposefully generate inaccurate or erroneous information. There is no mechanism for correcting this."[19] The agency unlawfully shifts responsibility for verifying the agency's information onto the social media users the agency plans to follow: "the community is largely self-governing and erroneous information is normally expunged or debated rather quickly by others within the community with more accurate and/or truthful information."[20] The users the agency is following will not even have notification that the agency will rely on the information they provide.[21]

---

[16] 6 U.S.C. §§ 121(d)(21)(A)-(B) (2010).

[17] System of Records Notice at 5603.
[18] 5 U.S.C. § 552a(e)(6).
[19] Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 9, June 22, 2010.
[20] *Id.*
[21] *Id* at 8.

Assuming autonomous, self-correcting processes do exist on the social media services the agency is targeting, including Myspace, Facebook, and YouTube, there is still no way to determine whether the agency is following individuals who expunge false information or the ones whose false information is expunged. The agency has glossed over this point with a brief mention of efforts to compare social media information with an unspecific "variety of public and government sources."[22] The agency fails to provide any affirmative technical or legal measures to exclude social media results that its agents or other social media users identify as inaccurate, incomplete, or irrelevant. The Department concedes that "there is no specific procedure for correcting information to DHS."[23]

DHS falsely states that this initiative will not "actively collect personally identifiable information (PII)."[24] In fact, the agency will actively collect PII "when it lends credibility to the report or facilitates coordination with federal, state, local, tribal, territorial, foreign, or international government partners."[25] The proposed initiative gathers personally identifiable information, including full names, affiliations, positions or titles, and account usernames.[26] Social media users also routinely provide a range of sensitive information in their online communications with no intention of submitting that information to the Department of Homeland Security. The agency anticipates retrieving such information in the normal course of performing social media searches.[27] DHS states that it will redact PII before "dissemination," presumably to other agencies as well as

[22] Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 5, Jan. 6, 2011..
[23] *Id.* at 11.
[24] System of Records Notice at 5603.
[25] *Id.* at 5603-4.
[26] *Id.* at 5604.
[27] *Id.* at 5603.

state, local, tribal, and foreign governments, and authorized private sector entities.[28] The agency does not state in the System of Records Notice whether it will actively erase PII before storing its own copies of the records. Such feeble privacy protections are simply inadequate.

DHS also alleges that the PII it collects will be de-identified prior to dissemination.[29] However, the content that DHS is collecting and compiling lends itself to common re-identification techniques. *The New York Times* has re-identified supposedly anonymous search engine queries released by AOL.[30] Bloggers set up websites to make it easier for the public to search the AOL data, which led to the re-identification of additional search records.[31] Additionally, researchers from the University of Texas found that if an adversary knows six precise ratings a person in the Netflix video-rental database has assigned to obscure movies, without any other information, the adversary can identify that person 84% of the time.[32]

2. DHS Must Narrow Its Proposal In Order to Comply With Its Statutory Authority

DHS's proposal requires a much narrower mission with clear oversight mechanisms and limiting guidelines. Congress did not grant or delegate direct intelligence gathering to DHS in the statutory provision cited by the agency as the

[28] *Id.* ("The NOC will . . . . disseminate relevant and appropriate de-identified information to federal, state, local, and foreign governments, and private sector partners authorized to receive situational awareness and a common operating picture.").
[29] *Id.*
[30] Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No.* 4417749, N.Y. TIMES. Aug. 9, 2006, at A1.
[31] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* 4 University of Colorado Law Legal Studies Research Paper No. 09-11 (2009).
[32] Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Datasets (How to Break the Anonymization of the Netflix Prize Dataset),* PROC OF 29TH IEEE SYMPOSIUM ON SEC. AND PRIVACY, Oakland, CA, 111-125 (May 2008).

primary authority for this program.[33] The cited provision enables the DHS Secretary to "*access*, *receive*, and *analyze* law enforcement information, intelligence information, and other information from agencies of the Federal Government, State and local government agencies and private sector entities," but not to *gather* information.[34] The only relevant provision that does mention gathering narrows the term to "incident management decisionmaking."[35] The contemplated data collection exceeds this statutory mandate.

Despite this limitation, DHS announced on June 22, 2010 that it would no longer restrict its intelligence gathering under the proposed program to individual incidents.[36] Previously, the agency issued Privacy Impact Assessments (PIAs) for social media monitoring connected to specific events on an incident per incident basis.[37] The DHS issued separate PIAs for the Haiti Social Media Disaster Monitoring Initiative, the 2010 Winter Olympics Social Media Event Monitoring Initiative, and the April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative.[38] PIAs play an important role in furthering Congress's mandate that new DHS programs do not "erode citizens' privacy"

---

[33] *See* Systems of Records Notice at 5604 ("DHS is authorized to implement this program primarily through 6 U.S.C. 121; 44 U.S.C. 3101; Executive Order (E.O.) 13388; OPS Delegation 0104; and Homeland Security Presidential Directive 5.").
[34] 6 U.S.C. § 121 (2010) (emphasis added).
[35] 6 U.S.C. § 321d(a) (2010) ("In this section, the term 'situational awareness' means information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management decisionmaking.").
[36] Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 5, June 22, 2010.
[37] Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Haiti Social Media Disaster Monitoring Initiative, January 21, 2010, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_haiti.pdf; Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning 2010 Winter Olympics Social Media Event Monitoring Initiative, February 10, 2010, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_2010winterolympics.pdf; Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative, April 29, 2010, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_bpoilspill.pdf.
[38] *Id*.

and ensure that agency activities are fully compliant with statutory privacy laws.[39] In June, DHS decided to discontinue its previous practice and instead issue semi-annual "overarching PIA[s]" for all of NOC's social media monitoring.[40]

In its System of Records Notice, the agency's justification for this change relies on statutory language that does not apply to ongoing information gathering initiatives. DHS is redeploying Congress's original stated purposes for establishing the NOC to justify its new, ongoing social media monitoring initiative. The agency stated that "[t]his system of records will allow DHS/OPS, including the NOC, to provide situational awareness and establish a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate."[41] Congress articulated these purposes when establishing the NOC but explicitly restricted the NOC's intelligence gathering authority to the requirements posed by specific events.[42] Congress refrained from granting independent gathering authority to the NOC on an ongoing basis.[43]

The purposes the NOC has proposed are overly broad and would authorize the collection of personal information on an ongoing basis for virtually any reason, or no reason at all. Moreover, DHS fails to mention any affirmative technical or legal measures to exclude social media results which do not meet its stated situational awareness goal. As currently described, this proposal violates the NOC's statutory grant of authority and imperils the privacy of millions of social media users.

3. DHS Should Conduct a Formal Rulemaking Process To Solicit Public Input

[39] 6 U.S.C. § 142 (2010).
[40] Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, 5, June 22, 2010.
[41] System of Records Notice at 5603. *See also* 6 U.S.C. 321d(b)(1)-(2).
[42] 6 U.S.C. §§ 321d(a), (b)(1)-(2)
[43] *See* 6 U.S.C. § 121.

In its February 1, 2011 System of Records Notice, DHS contradicts previous public statements and positions, establishing that the agency consciously refused to comply with Privacy Act requirements for soliciting public input. Before 2011, the agency conducted multiple social media monitoring initiatives without issuing a single System of Records Notice.[44] In June of 2010, DHS stated that "while the NOC may receive PII, PII is not actively collected and is not retrieved by personal identifier so a Privacy Act System of Records Notice is not required."[45] DHS stated in its February 1, 2011 System of Records Notice that its decision to store and disseminate PII in "life or death situations" had triggered the agency's legal obligation under the Privacy Act of 1974 to publish a System of Records Notice.[46] On January 6, 2011, the agency stated that "due to this new collection of PII and the ability of retrieval by personal identifier, a system of records notice (SORN) is now needed."[47] Internal documents dating back to 2009 demonstrate that the agency's "life or death" PII policy is longstanding.[48] A set of DHS slides released to the public in response to a Freedom of Information Act request detail the agency's social media monitoring efforts to "provide enhanced situational awareness" during preparations for the January 20, 2009 inauguration of President

[44] Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Haiti Social Media Disaster Monitoring Initiative, January 21, 2010, Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning 2010 Winter Olympics Social Media Event Monitoring Initiative, February 10 ,2010, Department of Homeland Ssecurity, Privacy Impact Assessment for the Office of Operations Coordination and Planning April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative, April 29, 2010; Department of Homeland Security, Privacy Impact Assessment for the Office of Operations Coordination and Planning Publicly Available Social Media Monitoring and Situational Awareness Initiative, June 22, 2010.
[45] Privacy Impact Assessment, June 22, 2010, 5.
[46] System of Records Notice at 5603.
[47] Privacy Impact Assessment, Jan. 6, 2011, 3.
[48] Social Network Monitoring Center Concept of Operations For the Presidential Inauguration, Electronic Frontier Foundation, *5, available at* https://www.eff.org/files/filenode/social_network/DHS_SNMC_Inauguration_monitoring.pdf

Barack Obama in Washington, D.C.[49] One of these slides states that DHS "will report PII information that relates to rare situations that have 'life or death' implications."[50] As this longstanding policy is clearly not the agency's motivation for issuing a System of Record Notice, it is reasonable to conclude that the agency knew of its legal obligations and simply failed to meet them.

DHS has also failed to comply with Administrative Procedure Act ("APA") requirements for soliciting public input. Before promulgating any rule, Section 553 of the APA requires agencies to provide the public with notice and opportunity to participate in the rulemaking "through submission of written data, views, or arguments."[51] DHS's Social Media Monitoring and Situational Awareness Initiative constitutes a rule, which the statute defines as "the whole or a part of an agency statement of general or particular applicability and future effect designed to implement, interpret, or prescribe law or policy or describing the organization, procedure, or practice requirements of an agency."[52] The proposed initiative is an agency statement describing a change in agency policy going forward. The System of Records Notice describes the agency's conduct as "launching" an ongoing social media monitoring program and developing a "new" system of records in the process. The program will have a significant future impact on the privacy rights of social media users whose accounts are monitored without their consent, stored in government databases, and disseminated across the country and overseas. The initiative therefore constitutes a rule, triggering statutory obligations under federal law to provide sufficient notice and opportunity for comment to the public.

---

[49] *Id.*
[50] *Id.* at 17.
[51] 5 U.S.C. §§ 553(b)-(c) (2010).
[52] 5 U.S.C. § 551(4) (2010).

Conclusion

For the foregoing reasons, EPIC recommends completely halting the agency's Social Media Monitoring Initiative. At minimum, EPIC recommends a comprehensive overhaul and full assessment of the privacy and security implications of the program under the federal Privacy Act. Such an overhaul must entail the following rudimentary measures to begin remedying the most blatant legal and policy flaws of the current proposal:

- Tether all social media monitoring efforts to the decisionmaking management requirements posed by individual events.
- Impose meaningful restrictions on gathering of information in lieu of the catch-all term "situational awareness."
- Provide meaningful notice to all individuals whose social media accounts the agency monitors.
- Narrow search terms to avoid retrieving potentially embarrassing information.
- Ensure the accuracy and relevance of all collected information.
- Develop affirmative measures to remove incorrect, incomplete, or irrelevant information.
- Provide individuals with meaningful opportunities to correct information gathered by the agency.
- Bolster administrative or physical safeguards that will ensure the confidentiality of these records.
- Do not communicate private information or Personally Identifiable Information via phone or email.
- Do not store or disseminate any Personally Identifiable Information.
- Provide public notice and opportunity for comment through an Administrative Procedure Act rulemaking.

Marc Rotenberg
EPIC Executive Director

Thomas H. Moore
Of Counsel

Conor Kennedy
Appellate Advocacy Fellow