epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE NATIONAL LIBRARY OF MEDICINE,
THE NATIONAL INSTITUTES OF HEALTH of
THE DEPARTMENT OF HEALTH AND HUMAN SERVICES

[FR Doc. 2013-08788]

NLM People Locator System 0925-0612
Notice of Proposed Collection

June 14, 2013

By notice published April 15, 2013,[1] in compliance with the Paperwork Reduction Act, the National Library of Medicine ("NLM"), National Institutes of Health ("NIH"), of the Department of Health and Human Services ("HHS") has proposed a public data collection, the People Locator System ("PLS"). The Paperwork Reduction Act mandates that, in connection with federal information collections, agencies "assume responsibility and accountability" for Privacy Act compliance and enforce privacy, confidentiality, and security "policies, procedures, standards, and guidelines."[2] Accordingly, pursuant to NIH's notice the Electronic Privacy Information Center ("EPIC") hereby submits these comments to address the substantial privacy and security issues raised by the PLS and to urge NIH to address these issues by restricting the collection, use, sharing, and retention of personally identifiable information ("PII") in the PLS. Specifically, EPIC recommends NIH: (1) limit the PLS information to relevant information, permit individuals

[1] Notice of Proposed Data Collection: NLM People Locator System, 78 Fed. Reg. 22271 (proposed Apr. 15, 2013) [hereinafter *PLS Notice*].
[2] 44 U.S.C. § 3506(g).

to amend their PLS records, and create a PLS auditing system; (2) implement access controls to PLS data; (3) limit the circumstances under which the agency will collect information and define a record retention and disposal schedule; (4) establish quality control standards; and (5) establish guidelines, which adhere to the Fair Information Practices, for third party disclosure.

NIH should issue a revised notice of proposed collection after incorporating public comments.

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. Since 2005, EPIC has advocated for HHS to build strong privacy protections into the systems it designs for individuals displaced or otherwise affected by disasters. In its 2005 comments to HHS on the State Parent Locator Service ("SPLS") for child support enforcement, EPIC emphasized the importance of enforcing strong database access rules and recommended requiring audit logs and accuracy provisions.[3] To support its claims, EPIC cited cases where innocent citizens were harmed as a result of unauthorized database use and inaccurate data entry.[4] In the 2007 comments to HHS on the National Disaster Medical System ("NDMS"), EPIC called for a strong, meaningful, and enforceable privacy to be built into NDMS in support of patient care and data integrity.[5] EPIC also implored HHS to comport with established medical privacy regulations and to protect the privacy of domestic violence survivors.[6] Among EPIC's specific recommendations, EPIC encouraged HHS to create an opt-in structure that would require patient notice and consent for any disclosure of location information.[7]

---

[3] EPIC et al., *Group Comments to HHS on "Parent Locator Databases"* (Dec. 13, 2005), *available at* http://epic.org/privacy/poverty/ocse121305.html.
[4] *Id.*
[5] EPIC, *Comments to HHS on National Disaster Medical System (NDMS) Patient Treatment and Tracking Records System (Docket No. HHS-2007-0159)*, at 3 (July 26, 2007), *available at* https://epic.org/apa/comments/EPIC-HHS-Med-Patient-Tracking.pdf.
[6] *Id.* at 8-10.
[7] *Id.*

Scope of the Proposed Collection

PLS and a related mobile app, ReUnite™, aim to support "the reunification of family members and friends who are separated during a disaster."[8] Both comprise NIH's intramural Lost Person Finder ("LPF") R&D project.[9] NIH hastened PLS development to assist with recovery following the January 2010 earthquakes in Haiti.[10] As proposed, PLS would compile a massive database of information describing missing or found individuals. PLS would gather data from "family members or loved ones"[11] and "first responders, volunteers, and other relief workers."[12] With PLS the NIH would also share personal information with third parties, including Google Person Finder, CNN, and the International Red Cross ("ICRC").[13] In the case of Google, during the Haiti relief efforts, the PLS freely shared data with Google Person Finder "to ensure that users of either system had access to as much relevant information as possible."[14]

PLS allows third parties to enter highly sensitive information about each missing or located individual, which in turn is accessed by the public. The system supports images, audio, maps, structured data, and image tagging.[15] Future planned changes include on-device data encryption and facial recognition.[16] Examples of disaster victims' PII recorded in PLS include: name, location, physical attributes, date of birth, race, religion, health status, address, photographs, voice recordings, social media URLs, general notes and comments.[17]

Frequently, disaster victims are displaced, traumatized, and dependent on the government for safety and basic necessities like food, water, shelter, and medical care. In this context, the

[8] *PLS Notice.*
[9] *Id.*
[10] David H. Sharlip, National Library of Medicine, *Supporting Statement A for NLM's People Locator System [DRAFT]*, Apr. 4, 2013 [hereinafter *PLS Supporting Statement*].
[11] *PLS Notice*.
[12] *PLS Supporting Statement*.
[13] National Library of Medicine Creates Haiti Earthquake People Locator, U.S. National Library of Medicine, http://www.nlm.nih.gov/news/people_finder.html.
[14] *PLS Supporting Statement*.
[15] *Id.*
[16] *Id.*
[17] *See, e.g.,* Department of Health and Human Services, *NLM's PEOPLE LOCATOR® Data Elements* (Apr. 2, 2013) [hereinafter *PLS Data Elements*].

timely exchange of accurate information among governmental and quasi-governmental relief entities is critical, and some forms of technology-enabled collection and use of PII are helpful and warranted. In many instances, however, particularly where private entities are involved, extensive collection and use of PII during and after a disaster is inappropriate and can result in extreme violation of victims' privacy.

Such a violation can expose already vulnerable individuals to mistake, fraud, humiliation, and abuse. Following Hurricanes Katrina and Sandy, domestic violence survivors, undocumented immigrants, and patients with HIV and mental health disorders faced formidable challenges in obtaining relief, sometimes electing to forego benefits in favor of safeguarding their own privacy and personal security.[18] Given such high stakes, NIH must carefully balance the need for reunification with the need to protect individual disaster victims' privacy interests.

With this proposed information collection, NIH invites public comment on "one or more of the following points":

> (1) Whether the proposed collection of information is necessary for the proper performance of the function of the agency, including whether the information will have practical utility; (2) The accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (3) Ways to enhance the quality, utility, and clarity of the information to be collected; and (4) Ways to minimize the burden of the collection of information on those who are to respond, including the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.[19]

[18] *See, e.g.,* Make the Road New York, *Unmet Needs: Superstorm Sandy and Immigrant Communities in the Metro New York Area*, at 5, 20 (Dec. 2012), *available at* http://www.maketheroad.org/report.php?ID=2550; Cynthia A. Bascetta, Director, Health Care, United States Government Accountability Office, Testimony Before the Ad Hoc Subcommittee on Disaster Recovery, Committee on Homeland Security and Governmental Affairs, U.S. Senate: *Hurricane Katrina: Barriers to Mental Health Services for Children Persist in Greater New Orleans, Although Federal Grants Are Helping to Address Them*, at 2 (July 13, 2009), *available at* http://www.gao.gov/assets/130/123199.html; Tulane University, Newcomb College Center for Research on Women, *Katrina and the Women of New Orleans*, at 66 (Dec. 2008), *available at* http://tulane.edu/nccrow/upload/NCCROWreport08.pdf; Ryan Singel, *Katrina Whips Up Data Storm*, Wired News, May 5, 2006, http://www.wired.com/politics/security/news/2006/05/70819.

[19] *PLS Notice*.

EPIC's recommendations pertain to points 3 and 4 above because by protecting privacy and information integrity, NIH can enhance the quality of information, as well as minimize the burden on respondents.

PLS Raises Substantial Privacy Issues

While PLS contains promising features to support the timely reunification of individuals after a disaster, it also raises many significant privacy issues that must be remedied as the agency continues to collect sensitive, identifying information. In order to address the privacy concerns that PLS data collection raises, EPIC recommends that NIH begin by adhering to the Privacy Act, Health Insurance Portability and Accountability Act ("HIPAA"), and Fair Information Practices when developing a privacy framework for PLS. Adherence to these privacy laws and standards will allow PLS to assist in the reunification of family members and friends during or after a natural disaster, without encroaching on the privacy rights of those intended to benefit from the system.

PLS enables the collection, use, and public dissemination of an extraordinary array of highly sensitive PII.[20] Furthermore, NLM plans to incorporate add-on technologies that will make the data even more powerful in the hands of those who possess it. Technologies for mapping, facial recognition, crowdsourced tagging, and other information retrieval functions, make PLS more than a simple bulletin board where people can post messages about their lost loved ones. PLS's data aggregation and processing capabilities exceed what is appropriate for a publicly shared federal database.

It is particularly troubling that NIH has instituted no specific safeguards to protect the privacy of vulnerable populations whose health, safety, or wellbeing might be inadvertently compromised as a result of PLS and its lack of privacy protection. These include children, survivors of domestic violence, patients with sensitive mental or physical health issues, and citizens exercising their rights to public benefits or due process. The inclusion, and public

[20] *See, e.g.*,*PLS Data Elements*.

dissemination, of location and health information could particularly imperil such parties. By definition, victims of disasters are in a state of heightened vulnerability. This state can be compounded by and also aggravate other pre-existing issues. Thus, collection and use of PII from vulnerable individuals necessitates special care and discretion.

Federal law recognizes the privacy interests inherent in such collection and use. For example, the Privacy Act requires an agency, where practicable, to collect information directly from an individual "when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs."[21] In order to reinforce the privacy standards outlined above when PLS is in operation, EPIC urges NLM to protect vulnerable populations by implementing the protections described below.

1) NIH Should Limit PLS information to Relevant Information, Permit Individuals to Amend their PLS Records, and Create a PLS Auditing System

The Privacy Act requires an agency to provide individuals opportunity to access and request amendments to records pertaining to them.[22] Because PLS data is entered by a wide array of users, including volunteers and the public, people must be able to request that NIH amend or delete records pertaining to them. NIH fails to specify how a party would make such a request. As EPIC President and Executive Director Marc Rotenberg has stated, where PII is collected and used absent a person's informed consent, it is vital that rights and responsibilities for that data be clearly allocated.[23] NIH has failed to allocate clearly rights and responsibilities for PLS data.

Due to the wide scope, disclosure, and storage of information collected by PLS, EPIC recommends that any personal data submitted to PLS without the explicit consent of the individual it relates to, should be limited to information that is relevant to the purposes for which it is to be used.

[21] 5 U.S.C. § 552a(e)(2) (1974).
[22] 5 U.S.C. § 552a(d) (1974).
[23] Marc Rotenberg, President, EPIC, Keynote Address at the Third International Summit on the Future of Health Privacy: *The Constitution & Privacy: Why the Supreme Court Cares* (June 5, 2013).

Additionally, EPIC recommends that PLS protect personal information, especially the data that it shares among partner organizations, with reasonable security safeguards against such risks as unauthorized use, disclosure, modification, or destruction. Details about the privacy framework protecting personal data in the PLS should be made available to the public. Further, NIH should include an auditing system where an individual would be able to request to see who has accessed his or her information in the PLS system, similar to the auditing system EPIC proposed in 2005 in comments regarding NIH's State Parent Locator Service.[24] Additionally, NIH should provide an opportunity for individuals to amend or remove any of their identifying information.

2) NIH Should Implement Access Controls to PLS Data

PLS is designed for use by two distinct groups of users: community laypersons—including family members and loved ones of missing individuals; and first responders, volunteers and other relief workers assisting in the disaster recovery effort.[25] Both groups have the ability to create new personal records, although it is unclear what specific permissions each group possesses, *e.g.*, who among them can modify, delete, or view full or restricted records. It is also unclear who manages those permissions and what qualifies a person for specific permissions. Particularly problematic is the fact that any member of the public with access to the Internet can view personal records.

The data access, oversight and accountability parameters expressed by NIH in its notice are unacceptably vague. Without more explicitly defined protocols, this essentially grants both read and write access to sensitive information to non-administrative users and is therefore excessively broad. EPIC urges NIH to clarify and narrow these parameters.

[24] EPIC et al., *supra* note 3.
[25] Privacy Office, Health and Human Services, Privacy Impact Assessment for NIH/NLM/iTunes/ReUnite, Aug. 9, 2011, *available at* http://www.hhs.gov/pia/TPWA%20PIA%20Summaries/nih_tpwa_summaries_fy12_q1.pdf.

For example, NIH must explicitly define who has membership to which groups and what their permissions are. NIH should segment data and structure in different tiers of access to PII collected by PLS. Such tiers should include giving volunteers and the general public read-only access to broad, non-sensitive data, and giving only licensed healthcare providers and/or relief workers read and write access to sensitive data. Additionally, NIH should implement a verification process for individuals who access the database's records. Such verification should then be cross-referenced with a municipal database of domestic violence complaints, in order to protect the privacy and safety of individuals in those situations.

3) NIH Should Limit the Circumstances Under Which it will Collect Information and Define a Record Retention and Disposal Schedule

NIH states that the system will "be activated only during times of declared emergencies, training and demonstration support activities, and would operate in declared emergencies until relief efforts have ceased in response to a particular disaster."[26] NIH must clearly define how and when an emergency is declared, as well as how and when relief efforts have ceased. In order to ensure that PLS does not become an overbroad collection of sensitive information, EPIC urges NIH to include in the operational guidelines a definition of "declared emergency." This definition is important to understand the scope of the proposed information collection.

Additionally, NIH does not specify how long records will be retained in PLS or in the systems of third parties. Long-term or indefinite retention of PII, particularly without notice or consent, would be inappropriate. Because many records will be created or updated without notice or consent, it would be inappropriate to retain data for any longer than necessary, even if for research purposes ordinarily authorized under HIPAA. NIH's ambiguity is problematic and must be clarified to prohibit record retention by any entities beyond a clearly defined period of disaster recovery. The privacy concerns implicated by the storing of nonconsensual health information far

[26] *PLS Notice*.

outweigh the research benefits that could be achieved, especially because there are other, consensual, ways to obtain such information.

4) NIH Should Establish Quality Control Standards

Under the Privacy Act, NIH has a responsibility to make reasonable efforts to assure that any records it provides to non-agency entities are "accurate, complete, timely, and relevant" for its purposes.[27] PLS includes some structured data fields.[28] These can afford greater data accuracy and consistency than free-text fields. However, it is unclear whether PLS has sufficient quality control standards for data. Because accountability for data entry and management is unclear, and because the system accommodates free text and multimedia files, NIH must define and enforce more explicit quality control protocols.

5) NIH Should Establish Guidelines, Which Adhere to the FIPS, for Third Party Disclosure

The Privacy Act[29] and the ICRC[30] discourage third party sharing of PII without an individual's informed consent. The ICRC specifies that without consent or a substantial public or individual interest, data should not be "used, disclosed, or transferred for purposes other than those for which they were collected without the consent of the person concerned."[31] PLS shares data with partners like Google Person Finder and ICRC, and it does not specify how it or its partners will collect, use, or share the information they gather, now or in the future. Nor does it clarify whether its partners follow FIPS.

Sharing data with third parties, particularly nongovernmental entities, exposes individuals to greater risk that their data will be out in the world and out of their control. EPIC finds troubling

[27] 5 U.S.C. § 552a(e)(6) (1974).
[28] *PLS Data Elements*.
[29] *See* 5 U.S.C. § 552a (1974).
[30] Int'l Comm. of the Red Cross, *Recommendations for the Development of a Domestic Law on the Missing and Their Families*, *in* The Missing and their Families: Summary of the Conclusions arising from the Events held prior to the International Conference of Governmental and Non-Governmental Experts (Feb. 19-21, 2003), *reprinted in* Joel R. Reidenberg et al., *Privacy and Missing Persons after Natural Disasters*, at 96, Ctr. on Law and Info. Policy, Fordham Univ. Sch. of Law and the Woodrow Wilson Int'l Ctr. for Scholars (2013) [hereinafter *ICRC Report*].
[31] *ICRC Report* at 96.

the absence of clear guidelines for current and future use of PII by PLS and its partners. PLS is a reunification service, not a direct provider of emergency medical care or disaster relief. As mentioned previously, it does not provide notice to individuals in its database. Thus, there is no compelling justification for it to share its data so freely.

The privacy issues raised above concerning PLS information collection, disclosure, and storage extend to the PLS partnerships with third parties such as Google, CNN, and the ICRC.[32] Therefore, EPIC urges NIH to require its partners to follow FIPS, which include the same privacy safeguards listed above, such as information collection with informed consent,[33] limited scope of information collection,[34] and prompt deletion of stored information after the emergency situation has ended.[35]

EPIC also urges NIH to include parameters as to the purposes for which personal data are collected, not later than at the time of data collection. The subsequent use of any collected information should then be limited to the fulfillment of those express purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.[36] This allows those disclosing personal data to know exactly for what purposes it will be used and also allows for a more comprehensible understanding of what data is relevant to the purposes of the collection. Additionally, personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with specified purpose, except with the explicit consent of the data subject or by the authority of law.

Conclusion

EPIC commends NIH for opening this discussion on the PLS and recognizes the utility of such a program. However, as outlined above, there are particular privacy interests that are

[32] National Library of Medicine Creates Haiti Earthquake People Locator, U.S. National Library of Medicine, http://www.nlm.nih.gov/news/people_finder.html.
[33] Federal Trade Commission, Fair Information Practice Principles, *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm.
[34] *Id*.
[35] *Id*.
[36] 5 U.S.C. § 552a(e)(10)(b) (1974).

implicated when personal data is being shared and stored, especially sensitive health and locational information. Therefore, to deal with these issues preemptively, EPIC recommends with this information collection, NIH, at a minimum: (1) limit its PLS information to relevant information, permit individuals to amend their PLS records, and create a PLS auditing system; (2) implement access controls to PLS data; (3) limit the circumstances under which it will collect information and define a record retention and disposal schedule; (4) establish quality control standards; and (5) establish Guidelines, which adhere to the Fair Information Practices, for third party disclosure.

Respectfully submitted,

Marc Rotenberg, EPIC President and Executive Director
Khaliah Barnes, EPIC Administrative Law Counsel
Elizabeth Hempowicz, EPIC Law Clerk
Heather Nodler, EPIC Law Clerk

Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue, NW Suite 200
Washington, DC 20009
(202) 483-1140 (tel)
(202) 483-1248 (fax)