COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS—2011—0074]

Notice and Request for Comment on ''The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research'' (''Menlo Report'') for the Department of Homeland Security (DHS), Science and Technology, Cyber Security Division (CSD), Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT)

February 27, 2012

By notice published on December 28, 2011, the Department of Homeland Security ("DHS") has invited the public to comment on "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research" ("Menlo Report") for the Department of Homeland Security ("DHS"), Science and Technology, Cyber Security Division ("CSD"), Protected Repository for the Defense of Infrastructure Against Cyber Threats ("PREDICT").[1] Specifically, the DHS S&T, CSD is interested in comments applicable to privacy issues and applicability of ethics with respect to human subjects in information and communication technology research ("ICTR").[2]

---

[1] Submission for Review and Comment: ''The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research'' (''Menlo Report'') for the Department of Homeland Security (DHS), Science and Technology, Cyber Security Division (CSD), Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT), 76 Fed. Reg. 81517 (proposed Dec. 28, 2011).

[2] *Id*.

The Electronic Privacy Information Center ("EPIC") submits these comments to reiterate legal obligations, established in the federal Privacy Act and other federal and states laws,[3] for government agencies that collect, use, and disclose personally identifiable information. While EPIC recognizes the need to provide ethical principles to guide ICTR, many federal privacy laws already provide guidelines and legal mandates about how government agencies can best protect individual privacy. When government agencies need guidance concerning ICTR privacy implications, they should first identify and apply binding federal privacy laws. In the absence of any conflict between the law and the Menlo Report, government agencies can adopt the Menlo Report principles. Contrary to the Menlo Report's argument, any conflict between Menlo Report principles and applicable law should be resolved in favor of upholding the law.

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 a particular interest in preserving privacy safeguards, established by Congress, in the development of new information systems operated by the federal government.[4] The ICTR discussed in the Menlo Report

---

[3] *See, e.g.,* The Privacy Act of 1974, 5 U.S.C. § 552a(2010); The Children's Online Privacy Protection Act, 15 U.S.C. § 6502 (2012); The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511 (2012); The Reader Privacy Act, CAL. CIVIL CODE § 1798.90 (2012); WASH. REV. CODE ANN. § 9.73.030 (2011); N.Y. CIV. RIGHTS LAW § 50-a (2011).

[4] *See, e.g.*, Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Notice of Privacy Act System of Records, Docket No. DHS-2011-0094 (Dec. 23, 2011), *available at* http://epic.org/privacy/1974act/EPIC-SORN-Comments-FINAL.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security, 001 National Infrastructure Coordinating Center Records System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2010-0086, DHS-2010-0085 (Dec. 15, 2010), *available at* http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of the

envisions the creation of new information systems. Additionally, EPIC has a particular interest in the privacy rights implicated by the Common Rule.[5] As discussed below, the Menlo Report is based on the Common Rule.

The Menlo Report

The Menlo Report is a proposal for a framework of "ethical guidelines for computer and information security research."[6] The intent of the report is to identify and resolve "ethical problems arising in research of or involving information and communication technology ("ICT")."[7] ICT is an "umbrella term that encompasses networks, hardware and software technologies that involve information communications pertaining to or impacting individuals and organizations."[8] ICT research ("ICTR") "involves the collection, use and disclosure of information and/or interaction with this ubiquitously connected network context which is overlaid with varied, often discordant legal regimes and social norms."[9] The Menlo Report is based on the 1979 Belmont Report, which provided guidelines for ethical research in the biomedical and behavioral sciences. The Belmont Report focused on three essential ethical principles for human

---

Electronic Privacy Information Center to the United States Customs and Border Protection; Department of Homeland Security on the Establishment of Global Entry Program, Docket No. USCBP-2008-0097 (Jan. 19, 2010), *available at* http://epic.org/privacy/global_entry/EPIC-Comments-Global-Entry-2010.pdf.

[5] EPIC: Privacy and The Common Rule, http://epic.org/privacy/privacy_and_the_common_rule.html; Comments of Professor Latanya Sweeney PhD, Director of the Data Privacy Lab of Harvard University, joined by the Electronic Privacy Information Center and 43 other privacy advocates, to the Department of Health and Human Services (Oct. 26, 2011), available at http://dataprivacylab.org/projects/irb/DataPrivacyResearchers.pdf.

[6] The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, p.2 (Sept. 15, 2011), *available at* http://www.cyber.st.dhs.gov/wp-content/uploads/2011/12/MenloPrinciplesCORE-20110915-r560.pdf.

[7] *Id*. at 5.

[8] *Id.*

[9] *Id*.

subject research: Respect of Persons, Beneficence, and Justice.[10] The Menlo Report adopts these three existing principles, and proposes to incorporate an additional principle: Respect for Law and Public Interest.[11]

The Belmont Report principles were incorporated and codified by the "Common Rule." Based partially on the Belmont Report, the Common Rule requires that "[f]ederally funded investigators in most instances obtain and document the informed consent of research subjects, and describes requirements for institutional review board (IRB) membership, function, operations, research review, and recordkeeping."[12] Since its inception, fifteen federal departments and agencies have codified the Common Rule in their agency regulations.

While the Common Rule focused on protecting human subjects of biomedical and behavioral, early ICTR "evolved without significant concern for human subjects, leading to instances where ethical considerations were either absent or misapplied because researchers failed to understand their relevant, or lacked any standards for assessment, accountability, or oversight."[13] The Menlo Report seeks to recognize human subject ethical considerations that were previously ignored in ICTR, including "stakeholders that

---

[10] The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, The National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research (April 18, 1979), *available at* http://ohsr.od.nih.gov/guidelines/belmont.html.
[11] The Menlo Report, p.2.
[12] Advance notice of proposed rulemaking: Human Subjects Research Protections: Enhancing Protections for Research Subjects and Reducing Burden, Delay, and Ambiguity for Investigators, Docket ID number HHS–OPHS–2011–0005, 76 Fed. Reg. 44512.
[13] The Menlo Report, p.6.

are non-research entities who rely on information and systems that are involved in the research and who may be harmed by its unavailability or corruption."[14]

Respect for Persons

Part C.2 of the Menlo Report addresses the Belmont Report's Respect for Persons principle. The Menlo Report states that

> [t]his principle has been applied by involving as research subjects only those with sufficient understanding or awareness to provide informed consent, or by obtaining in- formed consent from legally authorized representatives (e.g., parents of minors, relatives of unconscious patients, or guardians of those incapable of deciding for themselves). In the ICTR context, the principle of Respect for Persons includes consideration of the computer systems and data that directly interface, integrate with, or otherwise impact persons who are typically not research subjects themselves. [15]

The Menlo Report also outlines positive principles for obtaining informed consent, such as

> [i]nformed consent for one research purpose or use should not be considered valid for other research purposes. When an individual is identified with a group or organization, individual consent does not imply consent from other members of the group. Finally, informed consent for one research purpose or use should not be considered valid for different research purposes.[16]

However, the report states that "[w]here feasible, researchers should obtain informed consent to collect, use, or disclose sensitive identifying data, or to interact with information systems in ways that could negatively affect those systems or their users."[17] The report further states that "[t]here may be a conflict between satisfying ethical review requirements and separate legal protections . . . [w]hen a researcher believes waiver of

[14] *Id*. at 8.
[15] *Id*. at 9.
[16] *Id*. at 10.
[17] *Id*. at 9.

informed consent is warranted, he should clearly describe the justification for departing from the principle of consent."[18]

In the context of government ICTR, researchers are not authorized to waive consent because many federal privacy laws mandate that before collecting, using, or disclosing sensitive identifying data, government agencies must obtain individual consent. For example, the Privacy Act of 1974 forbids federal agencies from disclosing "any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[19] In certain limited circumstance, the Privacy Act permits disclosure of individual records without first obtaining individual consent. These circumstances, however, are narrowly prescribed and none of them involve simply providing "justification for departing from the principle of consent," as envisioned by the Menlo Report.[20] The Children's Online Privacy Protection Act ("COPPA") is another federal privacy law that agencies must comply with. Under COPPA, "[i]t is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child," to collect, use, or disclose the personal identifiable information of a child without obtaining parental consent.[21] The federal wiretap act, as amended by the Electronic Communications Privacy Act of 1986 ("ECPA") prohibits the unauthorized interception and disclosure of wire, oral, and electronic communications.[22]

---

[18] *Id*. at 10.
[19] 5 U.S.C. § 552a(b) (2010).
[20] *Id*. § 552a(b)(1)-(12); §552a(j)-(k).
[21] 15 U.S.C. § 6502 (a)-(b) (2012).
[22] 18 U.S.C. § 2511 (2012).

Agencies conducting ICTR also must comply with the Stored Communications Act ("SCA"), a federal privacy law that prohibits unauthorized access to "electronic communication while it is in electronic storage."[23] There are other federal privacy laws that would require ICT researchers to obtain a subject's consent before accessing or disclosing personally identifiable information.[24]

Thus, when applying the Menlo Report's Respect for Persons principle to government ICTR, government agencies are required by law to obtain research subjects' informed consent. Further, between a conflict among ethical review standards and legal obligations, government agencies must resolve the conflict in the favor of legal privacy protection.

Beneficence

Part C.3 of the Menlo Report incorporates the Belmont Report's Beneficence principle. The Beneficence principle encourages researchers to "do not harm" and "maximize possible benefits and minimize possible harms."[25] For the Menlo Report, "[t]ranslating this principle to ICTR demands a framework for systematic identification of risks and benefits for a range of stakeholders, diligent analysis of how harms are minimized and benefits are maximized, preemptive planning to mitigate any realized harms, and implementing these evaluations into the research methodology."[26] Federal agencies can adhere best to this principle through a privacy impact assessment ("PIA"). PIAs are of paramount importance and are mandated by federal law. Under the E-

---

[23]The Stored Communications Act, 18 U.S.C.A. § 2701.
[24] *See, e.g.*, The Video Privacy Protection Act of 1988, 18 U.S.C.A. § 2710 (2012); The Cable Communications Policy Act, 47 U.S.C. 521 *et seq*. (2012).
[25] The Belmont Report.
[26] The Menlo Report, p. 10.

Government Act of 2002, a federal government agency must conduct a PIA under the following circumstances:

> before (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or (ii) initiating a new collection of information that—(I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.[27]

Once those conditions are triggered, the agency is required to conduct a PIA:

> Each agency shall (i) conduct a privacy impact assessment; (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.[28]

The nature of ICTR is to collect, maintain, or disseminate personally identifiable information. Thus, in government ICTR, the Menlo Report's Beneficence principle should be understood to incorporate the legally mandated PIAs because PIAs establish clear guidelines in assessing privacy risks and mitigating privacy harms in ICTR.

Justice: Fairness and Equity

Part C.4 of the Menlo Report addresses the Belmont Report's Justice principle. The Menlo Report states that

> [i]n the Belmont Report, the principle of Justice is applied through fairness in the selection of research subjects, and equitable distribution of the burdens and benefits of research according to individual need, effort, societal contribution, and merit. In the ICTR context, this principle implies that research should not arbitrarily target persons or groups based on attributes including (but not limited to): religion, political affiliation,

[27] E-Government Act of 2002 § 208(b)(1)(A), 44 U.S.C. § 3501 (2008).
[28] *Id*. § 208(b)(1)(B).

> sexual orientations, health, age, technical competency, national origin, race, or socioeconomic status. Neither should ICTR target specific populations for the sake of convenience or expediency.[29]

Implicit in ICTR not selecting participants "for the sake of convenience of expediency," is ensuring that researchers adhere to privacy laws by obtaining consent to collect, use, or disclosure personally identifiable information. Researchers cannot collect or disclose a research subject's sensitive information without first obtaining consent, "for the sake of convenience or expediency."

Respect of Law and Public Interest

The Menlo Report states that its Respect for Law and Public Interest principle "is implicit in the Belmont Report's application of Beneficence" and that the principle encompasses "compliance and transparency and accountability."[30] Transparency is essential in the development of ethical guidelines because it is "a mechanism to assess and implement accountability, which itself is necessary to ensure that researchers behave responsibly."[31] Transparency in government ethical guidelines is especially necessary to ensure that government guidelines comply with federal laws. Additionally, the compliance component of this principle entails "due diligence to identify laws, regulations, contracts, and other private agreements that are applicable to . . . research."[32] Compliance should include ongoing obligations of data collectors, including but not limited to, utilizing information only for the purpose(s) for which it was gathered, safeguarding de-identified information against re-identification, and granting individuals a right of access and correction to their personal data.

---

[29] The Menlo Report, p.12.
[30] *Id*. at 13.
[31] *Id*. at 14.
[32] *Id*. at 13.

While the addition of the new Respect for Law and Public Interest principle is a positive addition to the Belmont principles, federal agencies already have legal obligations for transparency and accountability in their data systems. This mandatory compliance with federal privacy law supersedes the Menlo Report's Respect of Law and Public Interest. One of the concrete advantages of privacy laws over ethical guidelines is that privacy laws emphasize both the research interests and the corresponding legal implications. Privacy laws permit collection, disclosure, and use of personally identifiable information, under narrowly prescribed circumstances. These circumstances revolve around obtaining individual consent. On the other hand, guidelines tend to treat consent as the key variable and then ignore the interests of the data subject. Guidelines tend to favor research interests over privacy protection.

Additionally, the Menlo Report states that

> [i]f applicable laws conflict with each other or with the public interest, and a decision is made to not comply with legal obligations that are viewed as unethical, researchers should have ethically defensible justification and be prepared to accept responsibility for their actions and consequences.[33]

This statement is counterintuitive to compliance, transparency, and accountability. Adhering to the Menlo Report, researchers are permitted to make research decisions contrary to law, and are encouraged to "accept responsibility" for their actions. Should federal agencies adopt the Menlo Report to guide their ICTR, the agencies should not and cannot legally adopt this principle of knowingly violating federal laws for the sake of research.

---

[33] *Id*. at 14.

Conclusion

EPIC recognizes the Menlo Report's importance in establishing ethical principles to guide information and communication technology research. However, many of the report's principles and guidelines espouse violating federal privacy laws. Federal government agencies must first adhere to the legal principles and guidelines set forth by federal privacy laws before adhering to the Menlo Report.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Open Government Fellow

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)
barnes@epic.org