



TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



MACHINE-READABLE POLICIES

PIAs ♦ November 2009

Overview

Section 208 of the E-Government (E-Gov) Act of 2002 mandates the use of machine-readable privacy policies by Federal agencies on Web sites used by the public. Office of Management and Budget (OMB) Memorandum 03-22, “Guidelines for Implementing the Privacy Provisions of the E-Government Act of 2002,” outlines the privacy provisions of the E-Gov Act.

Requirement

OMB M-03-22 states that “agencies must adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences.” In addition, “agencies must develop a timetable for translating their privacy policies into a standardized machine-readable format” including “achievable milestones that show the agency’s progress toward implementation over the next year.” These timetables must be included in the annual E-Gov Act status reports sent to OMB.

What are machine-readable privacy policies?

Machine-readable privacy policies make use of the fact that Web browsers allow users to set their privacy preferences. Machine-readable policies are translated into a standard computer language that allows browsers to “read” these preferences and alert users if their site does not match their predetermined preferences.

What is P3P?

P3P stands for the Platform for Privacy Preferences Project and is the industry (and currently only) standard for machine-readable privacy policies. It consists of a standardized set of multiple-choice questions, covering all the major aspects of a Web site’s privacy policies. P3P-enabled Web sites make this information available in a standard, machine-readable format. P3P-enabled browsers can “read” this information automatically and compare it to the consumer’s own set of privacy preferences.

How does it work?

- 1) P3P allows Web sites to translate their privacy policies into a standardized, machine-readable format using Extensible Markup Language, or XML. This translation can be done manually or through automated tools. Once done, servers can be configured to enable the Web site to automatically inform visitors that it supports P3P.
- 2) P3P-enabled computers automatically fetch and read P3P privacy policies

piamail@tma.osd.mil ♦ www.tricare.mil/tma/privacy



TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



MACHINE-READABLE POLICIES

PIAs ♦ November 2009

on Web sites. P3P-equipped browsers can check privacy policies against the user's preferences or against other legal or regulatory guidelines. P3P client software can be built into a Web browser, plug-ins, or other software.

How does P3P help protect privacy?

Initial efforts by Web sites to publicly disclose their privacy policies have had some impact. But the burden has been on users to manually find, read and interpret narrative privacy policies. Machine-readable policies take Internet privacy efforts a step further. P3P places machine-readable privacy policies where browser applications can automatically and consistently find them and interpret them for the user. P3P assists Web users in deciding whether and under what circumstances to disclose personal information.

Who came up with this?

P3P was developed by the World Wide Web Consortium (W3C), an organization created in 1994 to promote collaboration and interoperability with regard to Internet standards. It is a non-profit, industry-supported consortium with over 400 member organizations, including corporations, research groups, non-profit organizations and governmental agencies around the world. Examples include Adobe Systems, Inc., AT&T, ChevronTexaco, Nokia, and Verisign, Inc.

What will P3P NOT do?

Machine-readable policies and P3P do not set minimum standards for privacy or provide a mechanism for ensuring that sites act according to their policies. Users should be aware that P3P does not protect privacy by itself. It is also not designed nor suited for addressing all critical elements of privacy protection. However, it does help create a framework for informed choice for consumers.

piamail@tma.osd.mil ♦ www.tricare.mil/tma/privacy



TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



MACHINE-READABLE POLICIES

PIAs ♦ November 2009

Additional Resources

World Wide Web Consortium: <http://www.w3.org>

W3C Platform for Privacy Preferences Initiative: <http://www.w3.org/P3P>

P3P Toolbox – resource developed to provide information on making Web sites P3P compliant: <http://www.p3ptoolbox.org>

GetNetWise – provides general information on using the Web and privacy issues, including privacy policies: <http://privacy.getnetwise.org>

W3C P3P Brochure: <http://www.w3.org/P3P/brochure.html>

“P3P and Privacy: An Update for the Privacy Community” by Ann Cavoukian PhD, Michael Gurski, Deirdre Mulligan, and Ari Schwartz. Center for Democracy and Technology. March 28, 2000. Available at: <http://www.cdt.org/privacy/pet/p3pprivacy.shtml>.

References

E-Government (E-Gov) Act of 2002, Section 208

OMB Memorandum 03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003

pia@mail@tma.osd.mil ♦ www.tricare.mil/tma/privacy