HEINONLINE

Citation: 7 Bernard D. Reams Jr. Law of E-SIGN A Legislative
of the Electronic Signatures in Global and National
Act Public Law No. 106-229 2000 iii 2002

Content downloaded/printed from
HeinOnline (http://heinonline.org)
Sun Apr 21 23:22:51 2013

-- Your use of this HeinOnline PDF indicates your acceptance
of HeinOnline's Terms and Conditions of the license
agreement available at http://heinonline.org/HOL/License

-- The search text of this PDF is generated from
uncorrected OCR text.

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Telecommunications, Trade and Consumer Protection, Committee on Commerce, House of Representatives

For Release on Delivery
Expected at
10 a.m. EDT
Wednesday,
October 11, 2000

INTERNET PRIVACY

Comparison of Federal Agency Practices With FTC's Fair Information Principles

Statement of Linda D. Koontz
Director, Information Management Issues





GAO-01-113T

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [iii] 2002

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [iv] 2002

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to discuss the privacy policies of selected federal web sites and their conformity with the Federal Trade Commission's four fair information principles—Notice, Choice, Access, and Security. After providing brief background information including an overview of the laws and guidance governing on-line privacy of federal web sites, my testimony today will discuss the findings in our recent report on Internet privacy which is based on the review we conducted at your request in July and August 2000.[1]

As you know, on-line privacy has emerged as one of the key—and most contentious—issues surrounding the continued evolution of the Internet. The World Wide Web requires the collection of certain data from individuals who visit web sites—such as Internet address—in order for the site to operate properly. However, collection of even this most basic data can be controversial because of the public's apprehension about what information is collected and how it could be used.

You asked us to determine how federal web sites would fare when measured against FTC's fair information principles for commercial web sites. In applying FTC's methodology, we analyzed a sample of 65 federal web sites to determine whether they collected personal identifying information, and if so, whether the sites included disclosures to indicate that they met the fair information principles of Notice, Choice, Access, and Security. We also determined the extent to which these sites allowed the placement of third-party cookies[2] and disclosed to individuals that they may allow the placement of these cookies. We did not, however, verify whether the web sites follow their stated privacy policies.

I should note that FTC staff expressed concern about this use of their methodology, stating that there are fundamental differences between federal and commercial web sites which, in their view, make FTC's methodology inappropriate for use in evaluating federal web site privacy policies. For example, an agency's failure to provide for Access or Choice on its privacy policy may reflect the needs of law enforcement or the

[1] *Internet Privacy: Comparison of Federal Agency Practices With FTC's Fair Information Principles* (GAO/AIMD-00-296R, September 11, 2000).

[2] A cookie is a small text file placed on a consumer's computer hard drive by a web server. The cookie transmits information back to the server that placed it, and, in general, can be read only by that server. A third-party cookie is placed on a consumer's computer hard drive by a web server other than the one being visited by the consumer-often without the consumer's knowledge.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 1 2002

dictates of the Privacy Act or other federal statutes that do not apply to sites collecting information for commercial purposes.

As of July 2000, all of the 65 web sites in our survey collected personal identifying information[3] from their visitors; 85 percent of the sites also posted a privacy notice. A majority of these federal sites (69 percent) met FTC's criteria for Notice. However, we found that a much smaller number of sites implemented the three remaining principles—Choice (45 percent), Access (17 percent), and Security (23 percent). Few of the federal sites—3 percent—implemented elements of all four of FTC's fair information principles. Finally, a small number of sites (22 percent) disclosed that they may allow third-party cookies; 14 percent actually allowed their placement.

Background

Concerned about the capacity of the on-line industry to collect, store, and analyze vast amounts of data about consumers visiting commercial web sites, the FTC reported in May 2000 on its most recent privacy survey of commercial web sites. The survey's objective was to assess the on-line industry's progress in implementing four fair information principles which FTC believes are widely accepted.

- Notice. Data collectors must disclose their information practices before collecting personal information from consumers.
- Choice. Consumers must be given options with respect to whether and how personal information collected from them may be used for purposes beyond those for which the information was provided.
- Access. Consumers should be able to view and contest the accuracy and completeness of data collected about them.
- Security. Data collectors must take reasonable steps to ensure that information collected from consumers is accurate and secure from unauthorized use.

In addition, the survey looked at the use of third-party cookies by commercial web sites. Although FTC noted improvement over previous surveys, it nonetheless concluded that the on-line industry's self-regulatory initiatives were falling short. As a result, a majority of the FTC

[3]Information used to identify or locate an individual, e.g., name, address, e-mail address, credit card number, Social Security number, etc.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 2 2002

commissioners, based on a 3 to 2 vote, recommended legislation to require commercial web sites not already covered by the Children's Online Privacy Protection Act (COPPA)[4] to implement the four fair information principles.

While the FTC's fair information principles address Internet privacy issues in the commercial sector, federal web sites are governed by specific laws designed to protect individuals' privacy when agencies collect personal information. The Privacy Act of 1974 is the primary law regulating the federal collection and maintenance of personal information maintained in a federal agency's systems of records.[5] The act provides, for example, that (1) agencies cannot disclose such records without the consent of the individual except as authorized by law, (2) under certain conditions, individuals can gain access to their own records and request corrections, and (3) agencies must protect records against disclosure and loss. While these requirements are generally consistent with FTC's fair information principles, the act's specific provisions limit the application of these principles to the federal government. Specifically, the Privacy Act applies these principles only to information maintained in a system of records and contains exceptions that allow, under various circumstances, the disclosure and use of information without the consent of the individual. On June 2, 1999, OMB provided additional guidance on Internet privacy issues in Memorandum M-99-18, directing agencies to post on principal federal web sites privacy policies that disclose what information is collected, why it is collected, and how it will be used. In a separate report issued earlier,[6] we evaluated selected federal web sites' privacy policies against certain aspects of applicable laws and guidance, and included a comparison of the Fair Information Principles and the Privacy Act. We also have ongoing work—which we intend to report on later this year—addressing in greater depth the use of cookies on federal web sites.

[4]15 U.S.C. 6501 et seq. The provisions of COPPA govern the collection of information from children under the age of 13 at web sites, or portions of web sites, directed to children or which have actual knowledge that a user from which they seek personal information is a child under 13 years old. These provisions took effect April 21, 2000.

[5]A system of records means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

[6]*Internet Privacy: Agencies' Efforts to Implement OMB's Privacy Policy* (GAO/GGD-00-191, September 5, 2000.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 3 2002

Scope and Methodology

As you requested, we used FTC's methodology to provide a snapshot of the privacy practices of two groups of web sites operated by executive branch agencies compared to the fair information principles. We reviewed a total of 65 sites during July 2000. One group consisted of web sites operated by 32 high-impact agencies, which handle the majority of the government's contact with the public.[7] A second group consisted of web sites randomly selected from the General Services Administration's (GSA) government domain registration database.[8] This group consisted mostly of web sites operated by small agencies, commissions, or programs. Finally, at your request, we assessed the FTC web site itself. (For the purpose of our analysis, the FTC site was added to the sites operated by the 32 high-impact agencies.)

In conducting our survey we generally followed the FTC methodology, including the selection of similar groups of web sites and the use of its data-collection forms and analytical techniques. We requested—and received—training from FTC similar to that provided to staff who collected and analyzed its survey information. Our staff underwent 2 half-days of training by FTC staff on its methodology and content analysis procedures for commercial web sites.

We visited the web sites in our samples from July 12 through July 21, 2000. We reviewed the web pages within the site—for up to a time limit of 15 minutes—to determine whether the site (1) collected any personal or personal identifying information, (2) posted a privacy statement, information practice statement, or disclosure notice, (3) provided individual access to and choice regarding use of the information, and (4) provided security over the information. We also looked for the placement and disclosure of third-party cookies.

[7]According to the National Partnership for Reinventing Government, these agencies handle 90 percent of the federal government's contact with the public.

[8]Our random sample was not large enough to project to the universe of federal web sites.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 4 2002

Federal Web Sites Surveyed Collect Personal Data But Vary in Degree of Conformity to FTC Principles

We found that all of the 65 web sites surveyed collected personal identifying information from their visitors. Most sites—85 percent—posted a privacy notice. However, they varied in the extent to which they provided Notice to consumers, allowed consumers Choice and Access regarding their information, disclosed that they provided Security for the information provided, and allowed and disclosed the placement of third-party cookies.

Using the same scoring methodology that FTC used for commercial sites, our survey showed that only 6 percent of the federal high-impact agencies and 3 percent of the randomly sampled sites federal web sites implemented, at least in part, each of the four fair information principles. The following explains how we scored the sites to determine conformance with each principle and describes how the federal web sites in our survey fared in conforming with each of the principles.

Notice

The Notice principle is a prerequisite to implementing the other principles. We concluded that a site provided Notice if it met all of the following criteria: (1) posted a privacy policy, (2) stated anything about what specific personal information it collects, (3) stated anything about how the site may use personal information internally, and (4) stated anything about whether it discloses personal information to third parties. Our survey showed that 69 percent of all sites visited met FTC's criteria for Notice.

Choice

Under the Choice principle, web sites collecting personal identifying information must afford consumers an opportunity to consent to secondary uses of their personal information, such as the placement of consumers' names on a list for marketing additional products or the transfer of personal information to entities other than the data collector. Consistent with such consumer concerns, FTC's survey included questions about whether sites provided choice with respect to their internal use of personal information to send communications back to consumers (other than those related to processing an order) and whether they provided choice with respect to their disclosure of personal identifying information to other entities, defined as third-party choice.

We concluded that a site provided Choice if both internal choice with respect to at least one type of communication with the consumer and third-party choice with respect to at least one type of information were given to individuals. Our survey showed that 45 percent of all sites met FTC's criteria for Choice.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 5 2002

Access	Access refers to an individual's ability both to access data about himself or herself—to view the data in the web site's files—and to contest that data's accuracy and completeness. Access is essential to improving the accuracy of data collected, which benefits both data collectors who rely on such data and consumers who might otherwise be harmed by adverse decisions based on incorrect data. FTC's survey asked three questions about Access: whether the site stated that it allows consumers to (1) review at least some personal information about them, (2) have inaccuracies in at least some personal information about themselves corrected, and (3) have at least some personal information deleted. We concluded that a site provided Access if it provided any one of these disclosures. Our survey showed that 17 percent of all sites met the FTC criteria for Access.
Security	Security refers to the protection of personal information against unauthorized access, use, or disclosure, and against loss or destruction. Security involves both management and technical measures to provide such protections. FTC's survey asked whether sites disclose that they (1) take any steps to provide security, and if so, whether they (2) take any steps to provide security for information during transmission, or (3) take any steps to provide security for information after receipt. We concluded that a site provided Security if it made any disclosure regarding security. Our survey showed that 23 percent of all sites met FTC's criteria for Security.
Third-Party Cookies	FTC defines a third-party cookie as a cookie placed on a consumer's computer by any domain other than the site being surveyed. Typically, in the commercial environment, the third party is an on-line marketing organization or an on-line service that tracks and tabulates web-site traffic. However, some federal web sites also allow placement of third-party cookies. Our survey showed that 22 percent of all sites disclosed that they may allow third-party cookies and 14 percent allowed their placement. Mr. Chairman, this concludes my statement. I would be happy to respond to any questions that you or other members of the Subcommittee may have at this time.

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 6 2002

Contact and Acknowledgements

For information about this testimony, please contact Linda D. Koontz at (202) 512-6240 or by e-mail at *koontzl.aimd@gao.gov*. Individuals making key contributions to this testimony include Ronald B. Bageant, Scott A. Binder, Mirko J. Dolak, Michael P. Fruitman, Pamlutricia Greenleaf, William N. Isrin, Michael W. Jarvis, Kenneth A. Johnson, Glenn R. Nichols, David F. Plocher, Jamie M. Pressman, and Warren Smith.

(301302)

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 7 2002

Ordering Information

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) 8 2002

Document No. 180

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [i] 2002

HeinOnline -- 7 Bernard D. Reams, Jr., Law of E-SIGN: A Legislative History of the Electronic Signatures in Global and National Commerce Act, Public Law No. 106-229 (2000) [ii] 2002