[Billing Code: 6750-01P]

FEDERAL TRADE COMMISSION

Privacy Act of 1974; System of Records

AGENCY: Federal Trade Commission (FTC).

ACTION: Notice of routine use.

SUMMARY: The FTC is adopting in final form a new routine use that permits disclosure of FTC records protected by the Privacy Act when reasonably necessary to respond and prevent, minimize, or remedy harm that may result from an agency data breach or compromise.

DATES: The routine use is effective [INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].

FOR FURTHER INFORMATION CONTACT: Alex Tang, Attorney, FTC, Office of General Counsel, 600 Pennsylvania Ave. NW, Washington, DC 20580, 202-326-2447, atang@ftc.gov.

SUPPLEMENTARY INFORMATION: In a document previously published in the FEDERAL REGISTER, 72 FR 14814 (Mar. 29, 2007), the FTC, as required by the Privacy Act of 1974, 5 U.S.C. 552a, sought comments on a proposed new "routine use" of the FTC's Privacy Act records systems.[1] As the FTC explained, the new routine use,

[1] The FTC simultaneously provided OMB and the Congress with 40 days advance notice of the proposed routine use, as required by the Privacy Act, 5 U.S.C. 552a(r), and OMB Circular A-130, Revised, Appendix I.

the text of which is set forth at the end of this document,[2] is necessary to allow for disclosures of Privacy Act records by the FTC to appropriate persons and entities for purposes of response and remedial efforts in the event of a breach of data contained in the protected systems. The routine use will facilitate an effective response to a confirmed or suspected breach by allowing for disclosure to individuals affected by the breach, in cases, if any, where such disclosure is not otherwise authorized under the Act. The routine use will also authorize disclosures to others who are in a position to assist in response efforts, either by assisting in notification to affected individuals or otherwise playing a role in preventing, minimizing, or remedying harms from the breach. The FTC explained that this new routine use would be added to Appendix 1 of the FTC's Privacy Act system notice; that Appendix describes the routine uses that apply globally to all FTC Privacy Act records systems.[3]

The Privacy Act authorizes agencies, after public notice and comment, to adopt routine uses that are compatible with the purpose for which information subject to the Act has been collected. 5 U.S.C. 552a(b)(3); see also 5 U.S.C. 552a(a)(7). The FTC believes that it is consistent with the agency's collection of information pertaining to individuals under the Privacy Act to disclose such records when, in doing so, it will help prevent, minimize or remedy a data breach or compromise that may affect such individuals. By

---

[2] The text of the routine use was taken from the routine use that has already been published in final form by the Department of Justice after public comment. See 72 FR 3410 (Jan. 25, 2007).

[3] See 57 FR 45678 (1992), http://www.ftc.gov/foia/sysnot/appendix1.pdf. A list of the agency's current Privacy Act records systems can be viewed on the FTC's web site at: http://www.ftc.gov/foia/listofpasystems.htm.

contrast, the FTC believes that failure to take reasonable steps to help prevent, minimize or remedy the harm that may result from such a breach or compromise would jeopardize, rather than promote, the privacy of such individuals.

In seeking public comments on the proposed routine use, the FTC explained that it would take into account any such comments and make appropriate or necessary revisions, if any, before publishing the proposed routine use as final. In response, the FTC received one comment, from the Electronic Privacy Information Center (EPIC).[4]

First, EPIC urges that the FTC narrow the proposed routine use to the minimum required to fulfill the agency's stated purpose. EPIC questions what standards or requirements the agency would follow in determining the Privacy Act disclosures to be made in the case of a data breach, and wonders whether the agency would now be routinely disclosing Social Security numbers or other sensitive personal information to other agencies, entities and persons in every data breach investigation. Recognizing that specific disclosures may be necessary, EPIC suggests, for example, that the FTC could create tiers of access, allowing specific categories of individuals limited access to data, according to the needs of the agency's investigation.

The FTC agrees that any disclosure of Privacy Act records in order to investigate or remedy a breach must be necessary and narrowly tailored to the circumstances. The FTC believes that the restriction on disclosures to those that are "reasonably necessary" accurately and appropriately describes the relevant limitation on disclosures under this routine use. The scope of potential disclosures authorized by that routine use is not

---

[4] See http://www.ftc.gov/os/publiccomments.shtm (#207).

intended to suggest that the FTC will always disclose all of an individual's records, if any, every time there is a breach that the agency needs to investigate or mitigate. Rather, the purpose and intent of the routine use is to give individuals full and fair notice of the extent of potential disclosures, consistent with the Privacy Act's requirement that individuals be made aware of how their records may be disclosed, even if the FTC anticipates that there may often be very limited or no disclosure of an individual's records to third parties as part of the agency's investigatory or remedial efforts.

Developing fixed categories of access for certain entities or individuals, as EPIC suggests, would not appear to confer significantly greater protection, if any, for an individual's records than limiting disclosures to those that are "reasonably necessary." The determination of when disclosure is "reasonably necessary" will logically depend on a case-by-case evaluation of the specific circumstances of the breach, including how much of an individual's information, if any, it is reasonably necessary to disclose, and the specific nature of the entities to whom such information needs to be disclosed, in order to investigate or respond to a breach.[5] Amending a routine use to accommodate disclosures in response to a breach on a case by case basis is not a viable option when there is a clear need to respond rapidly and effectively in investigating and mitigating the breach, in light of the prior notice and comment requirements of the Privacy Act for routine use amendments.

---

[5] For example, under FTC rules, disclosures to other law enforcement agencies may be made on a confidential basis for law enforcement purposes. See Commission Rule 4.11(c), 16 CFR 4.11(c).

Second, EPIC's comment advocates that consumers be notified as soon as possible after a security breach results in their personal information being accessed by an unauthorized person, and before notifying any other agency, entity or individual. That issue, however, is outside the scope of a routine use notice under the Privacy Act. The Act requires that agencies notify individuals about the establishment of a Privacy Act system of records, the routine uses of such systems of records, and additional notice at the time that information in such a system is collected from individuals.

Nothing in the Act, however, governs or provides criteria for determining when notice of a data breach to affected individuals would be appropriate or not. Guidance on that issue has been issued to all Federal agencies by the Office of Management & Budget (OMB), in conjunction with the President's Identity Theft Task Force, chaired by the Attorney General and co-chaired by the FTC Chairman.[6] As stated in that guidance, agencies must consider various factors in determining whether notice is appropriate in a given case. The routine use published by the FTC neither addresses nor is it intended to supersede or supplant such guidance, or any other applicable guidance that may later arise in applicable statute, rule or policy regarding when notice to individuals must or should be given.

---

[6] See Memorandum for the Heads of Department and Agencies, from Clay Johnson, Deputy Director for Management, OMB, "Recommendations for Identity Theft Related Data Breach Notification" (Sept. 20, 2006) (attaching Memorandum from the Identity Theft Task Force, "Identity Theft Related Data Security Breach Notification Guidance" (Sept. 19, 2006), also reproduced in The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan (Apr. 2007) at 73-82 (App. A)).

Accordingly, after consideration of the above, the FTC has determined to adopt the routine use for data breach as originally published, and hereby amends Appendix 1 of its Privacy Act system notices, as published at 57 FR 45678, by adding the following new routine use at the end of the existing routine uses set forth in that Appendix:

* * *

To appropriate agencies, entities, and persons when (1) the FTC suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the FTC has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the FTC or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the FTC's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

By direction of the Commission.

Donald S. Clark
Secretary