Memorandum

To: Interested Persons

From: Barry Steinhardt (ACLU)

Date: February 2, 2004

Re: The Power of the US Government Obtain Private Records

The EU -US agreement on the transfer of air passenger data purports to limit the use of the PNR data, when combined with other privately held data, which will be obtained" only through lawful channels".

Additional personal information sought as a direct result of PNR data will be obtained from sources outside the government only through lawful channels, and only for legitimate counterterrorism or law enforcement purposes. For example, if a credit card number is listed in a PNR, transaction information linked to that account may be sought, pursuant to lawful process, such as a subpoena issued by a grand jury or a court order, or as otherwise authorized by law. In addition, access to records related to e-mail accounts derived from a PNR will follow U.S. statutory requirements for subpoenas, court orders, warrants, and other processes as authorized by law, depending on the type of information being sought; (paragraph 6).

Aside from the little comfort that passengers from Europe, which will include Americans traveling back to the US, can glean from a promise that the US Government will act in a "lawful" manner-- was the alternative that they could obtain the data unlawfully-- the government power to obtain private data is actually very broad and there are very few protections or procedures built into the law.

Below is a short description of the legal authority of the US Government to obtain financial and medical information from US Sources:

Medical records-specific laws

Federal law enforcement agents in the United States have tremendous authority to seize personal medical information without a warrant. Regulations created pursuant to the Health Insurance Portability and Accounting Act of 1996 (HIPAA) provide a wide variety of circumstances under which medical information can be disclosed for law enforcement-related purposes without explicitly requiring a warrant.[1] These circumstances include (1) law enforcement requests for information to identify or locate a suspect, fugitive, witness, or missing person, (2) instances where there has been a crime committed on the premises of the covered entity, and (3) in a medical emergency in connection with a crime.[2]

The regulations also contain two separate subsections that specifically permit the release of private medical information for "National security and intelligence activities" as well as "Protective services for the President and others." One of these subsections states that a "covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act."[3] The other subsection allows analogous disclosures in order to protect the President, former Presidents, Presidents-elect, foreign dignitaries and other VIPs.[4]

Financial records-specific laws

In addition, law enforcement agents have wide ranging powers to collect personal financial information.

During the past few decades, banks have systematically reported a variety of customer transactions to the government in compliance with laws like the Federal Bank Secrecy Act. The Supreme Court ruled in *United States v. Miller*, that individuals do not have a "reasonable expectation of privacy" under the Fourth Amendment in financial records pertaining to them but maintained by a bank in the normal course of business.[5]

With limited exceptions including the Right to Financial Privacy Act enacted in 1978, Congress has consistently limited rather than expanded financial privacy.[6] In 1992 Congress amended the Bank Secrecy Act to authorize the Treasury Department to adopt the Suspicious Activity

---

[1] 45 C.F.R. § 164.512 (2002).
[2] Id. at 164.512 (f).
[3] 45 C.F.R. 164.512(k)(2).
[4] 45 C.F.R. § 164.512(k)(3).
[5] 425 U.S. 435 (1976); see also California Bankers Assoc. v. Shultz, 416 U.S. 21 (1974) (upholding the then limited reporting requirements of the Bank Secrecy Act. ACLU was a plaintiff in this case).
[6] 12 U.S.C. § 3401 et seq.

Reporting requirements,[7] mandating the Treasury Department to report any "suspicious transaction relevant to a possible violation of law or regulation."[8] At the same time, Congress completely insulated financial institutions from civil liability for reporting their customers as "suspects" to the government, and barred financial institutions from telling their customers that their bank had spied on them by reporting their transactions.

The Right to Financial Privacy Act is riddled with loopholes, including a significant requirement that the Act accommodate financial institution reporting under the Bank Secrecy Act.[9] Though the Right to Financial Privacy Act contemplates that notice will be given customers when financial records are transferred from one federal agency to another notice is not given when Suspicious Activity Reports are furnished to law enforcement officials.[10]

More recently, the Gramm-Leach-Bliley Act of 1999 requires all financial institutions (companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance) disclose any nonpublic personal information "for an investigation on a matter related to public safety"[11] or "to comply with Federal, State, or local laws, rules, and other applicable legal requirements; to comply with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law."[12]

USA Patriot Act

Finally, the government can also get access to personal medical and financial information through the USA Patriot Act. Notably, Section 215 of the Patriot Act allows the FBI Director or his designee to get a court order under the Foreign Intelligence Surveillance Act "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the

---

[7] The Annunzio-Wylie Anti-Money Laundering Act Title XV of P.L. 102-550, 106 Stat. 4044, 4059.
[8] 31 U.S.C. § 5318(g)(1).
[9] "Nothing in this chapter shall authorize the withholding of financial records of information required to be reported in accordance with any Federal statute or rule promulgated thereunder." 12 U.S.C. § 3413(d).
[10] 12 U.S.C. Section 3412(b).
[11] 15 U.S.C. § 6802(e)(5).
[12] Id. at §6802(e)(8).

Constitution."[13] This power clearly applies to medical and financial records. Last December, the FBI was given expanded authority under the Patriot Act to obtain personal information from banks, insurance companies, travel agencies, real estate agents, stockbrokers, the U.S. Postal Service, jewelry stores, casinos, and car dealerships without a warrant—all through a revised definition that treats such organizations as "financial institutions."[14]

European passenger data that is shared with the United States will receive little or no protection. Individuals targeted for scrutiny by U.S. officials will have no recourse as their most personal medical and financial is examined and processed in ways they never imagined and never contemplated when they purchased an airline ticket.

We urge the European Commission on Privacy to state that United States laws are not adequate to safeguard the privacy rights of European citizens and block the implementation of this proposed privacy sharing agreement.

Sincerely,

[13] 50 U.S.C. § 501(a)(1) (2002).
[14] 12 U.S.C. § 3414 (d) (2004).