February 20, 2004

Joshua B. Bolten
Director, Office of Management and Budget
725 17th Street NW
Washington, DC 20503

Dear Mr. Bolten:

In April we sent a letter to former OMB Director Mitchell E. Daniels, Jr. on behalf of nearly ninety organizations across the United States regarding the Justice Department's decision to discharge the Federal Bureau of Investigation of its statutory duty to ensure the accuracy and completeness of criminal records maintained in the National Crime Information Center (NCIC) database (attached hereto). To date no action has been taken on this request. We now respectfully urge the OMB to exercise its power pursuant to 5 U.S.C. § 552(r) to review the FBI's March 24, 2003 Privacy Act Notice published in the Federal Register and to revise the final rule to make the NCIC comply with crucial Privacy Act requirements.[1] This action is urgently needed to ensure the integrity of criminal justice records and to protect the privacy of millions of individuals, particularly because NCIC access and functionality continue to expand.

The NCIC is the most extensive system of criminal history records in the United States, containing information on more than 52 million individuals[2] and averaging 3.5 million transactions a day.[3] An NCIC profile typically contains an individual's name, address, date of birth, Social Security number, sex, race, and physical characteristics, and may also include place of employment, automobile registration, fingerprints, criminal history information, and juvenile record information, among other identifiers.[4]

A 2001 Bureau of Justice Statistics (BJS) study of NCIC found that "name searches of the NCIC are not fully reliable and existing criminal record files may be

---

[1] This final rule also exempted the Central Records System and National Center for the Analysis of Violent Crime systems from accuracy requirements of the Privacy Act. Privacy Act of 1974; Implementation, 68 Fed. Reg. 14140 (Mar. 24, 2003) (codified as 28 C.F.R. pt. 16).

[2] Federal Bureau of Investigation, *Protecting American Streets: Law Enforcement Information Sharing is Key* (Jan. 7, 2004), *available at* http://www.fbi.gov/page2/jan04/cjis010704.htm.

[3] Federal Bureau of Investigation, *Facts and Figures 2003*, *Law Enforcement Support, available at* http://www.fbi.gov/libref/factsfigure/lawenforce.htm.

[4] Bureau of Justice Statistics, Department of Justice, *Use and Management of Criminal History Record Information: A Comprehensive Report*, *2001 Update*, NCJ 187670 at 28-29 (Dec. 2001), *available at* http://www.ojp.usdoj.gov/bjs/pub/ascii/umchri01.txt.

incomplete or inaccurate, particularly with respect to case disposition information."[5] The BJS stated that when incomplete or inaccurate records are used, "there is a substantial risk that the user will make an incorrect or misguided decision."[6] The study concluded that "inadequacies in the accuracy and completeness of criminal history records is the single most serious deficiency affecting the Nation's criminal history record information system."[7]

Despite these recognized weaknesses, the FBI published in March 2003 a Federal Register notice and final rule[8] announcing that the NCIC will be exempt from a provision of the Privacy Act that requires an agency to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination[.]"[9] In addition to the objections to this exemption voiced in our April 2003 letter to OMB Director Daniels, there are new developments to which we would like to draw your attention that underscore the need for the NCIC to be subject to the accuracy requirements of the Privacy Act.

The NCIC is used in the Department of Homeland Security's vast border security program. The United States Visitor and Immigrant Status Indicator Technology (US-VISIT), recently launched at 115 airports and 15 seaports, uses information from NCIC and other sources to determine whether visitors traveling to the United States will be permitted into the country.[10] Inaccuracies in the NCIC database will likely undermine the effectiveness of this system, resulting in the erroneous designation of individuals as requiring additional scrutiny, failure to identify individuals that should legitimately not be permitted into the country, or perhaps even denial of innocent persons entry into the United States.

Another government initiative that may potentially make use of NCIC is the Computer Assisted Passenger Prescreening System (CAPPS II) currently under development by the Transportation Security Administration (TSA). CAPPS II was originally intended for aviation security purposes, but TSA has indicated that the system will also be used as a law enforcement tool and may eventually be linked with US-VISIT and used to help combat illegal immigration.[11] A recent General Account Office report on CAPPS II noted that "implementing these possible changes could require integration with other data systems, such as the National Crime Information

---

[5] *Id*. at 21.

[6] *Id*. at 38.

[7] *Id*.

[8] 68 Fed. Reg. 14140.

[9] 5 U.S.C. § 552(e)(5).

[10] Department of Homeland Security, *US-VISIT Program, Increment 1, Privacy Impact Assessment* at n.2 (Dec. 18, 2003), *available at* http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0333.xml.

[11] Interim Final Privacy Act Notice, 68 Fed. Reg. 45265, 45266 (August 1, 2003); General Accounting Office, *Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges*, GAO-04-385 at 29 (Feb. 2004), *available at* http://www.gao.gov/new.items/d04385.pdf [hereinafter *Aviation Security*].

Center[.]"[12] The agency has, however, acknowledged the database's known weaknesses: "TSA officials stated that some of these databases have reliability concerns, including the National Crime Information Center database."[13]

In addition to the danger the NCIC's inaccuracy presents to other government information technology programs, the FBI has recently expanded the NCIC to contain information indicating when a DNA profile of an individual exists in the Combined DNA Index System Program (CODIS), the FBI's DNA profile database.[14] One federal appellate court has already rejected the routine collection of DNA for CODIS citing privacy concerns.[15] The addition of DNA information to NCIC's records illustrates that the NCIC is expanding in scope, assimilating information it was never contemplated at its creation to include. The growth of NCIC can only exacerbate the database's inaccuracy problems.

The OMB has failed to address the FBI's exemption of the NCIC from Privacy Act accuracy requirements. For the reasons outlined above and those set out in the letter we sent in April, we respectfully request that the OMB evaluate the effect of the FBI's decision to exempt NCIC from 5 U.S.C § 552(e)(5) on criminal justice record integrity and the privacy rights of individuals, and require the FBI to reverse its rule.

Sincerely,

Marc Rotenberg
Executive Director

Marcia Hofmann
Staff Counsel

Enclosure

---

[12] *Aviation Security* at 29.

[13] *Id.*

[14] *See* National Institute of Justice, *Transcripts of the Attorney General's Initiative on DNA Laboratory Backlogs (AGID-LAB) Working Group, Integrating Systems* (Oct. 21, 2002), *available at* http://www.ojp.usdoj.gov/nij/dnainitiative/b12.html; Criminal Justice Info. Servs. Div. of the FBI, *National Crime Information Center (NCIC) Technical and Operational Update (TOU)* 03-3, at 2-5 (July 28, 2003), *available at* http://www.acjic.state.al.us/documents/TOU/tou03-3.pdf.

[15] *United States v. Kincade*, 345 F.3d 1095 (9th Cir. 2002), *reh'g en banc granted*, No. 02-50380, 2004 U.S. App. LEXIS 89 (9th Cir. 2004).