

FinCEN
P.O. Box 39
Vienna, VA 22183-0039

Submitted by email regcomments@fincen.treas.gov

Attention: Revisions to PA Systems of Records—Comments

We are writing to comment on the proposed changes to the Suspicious Activity Report System (the “SAR System”). Our primary concerns relate to the unintended consequences to privacy as a result of these changes.

Prior to the federal anti-money laundering statutes, common law expectations of privacy and marketplace competition inhibited the gratuitous sharing and selling of previously private, personal financial information. The adoption of the Bank Secrecy Act three decades ago inadvertently ushered in a serious deterioration of consumer financial privacy. In 1976, the U.S. Supreme Court held in *Miller v. United States* that depositors have “no legitimate ‘expectation of privacy’” in their bank records since the information could be passed from the other person to the government (as required by the Bank Secrecy Act).

As a result of the change in expectations, Congress passed the Right to Financial Privacy Act in 1978 that reinstated limited expectations of privacy. Unfortunately, the protections were not strong enough. Today, the loss of an individual’s control over their financial information is a serious issue. Identity fraud, enabled through the Bank Secrecy Act ramifications, has contributed to an epidemic of identity theft. The Suspicious Activity Report (SAR) changes proposed may exacerbate that problem.

Pursuant to the 2001 National Money Laundering Strategy, FinCEN should now establish a system to evaluate objectively a public strategy regarding the new uses of the SARs and how they will be proven most effective. What are the measurable goals? What are the criteria and means to evaluate objectively how well the goals are reached?

Should the new uses of the SARs fail to measure up to the articulated goals, we agree with the assessment of the Strategy, “If anti-money laundering initiatives are not making a significant difference in disrupting money laundering activity, principles of good government mandate that law enforcement discontinue those efforts.”

While we support the efforts of the federal law enforcement officials to prevent and investigate acts of terrorism, we are concerned that the new changes may deluge officials with unnecessary information that will divert resources from more productive uses. Efforts should be made to reduce the amount of information

collected and increase its usefulness. Since there is little indication of terrorists using Nevada casinos to fund their activities, we oppose the extension of SAR requirements for Nevada casinos.

Under the current Bank Secrecy Act, between 1987 and 1996, 77 million Currency Transaction Reports (CTRs) were filed. Of those, 7300 defendants were charged, with only 580 ending up in conviction. Furthermore, between 1994 and 1998, the number of persons charged with money laundering as a result of Suspicious Activity Reports (SARs) fell by more than 24%, according to the Transactional Records Access Clearinghouse.

Data Retention

One of the best privacy safeguards is to minimize the collection of personal data where possible. We applaud the plans to establish a highly secure network. Further efforts should be made to encourage the use of encryption and other privacy-protecting technologies regarding the transmittal of sensitive, personally-identifiable information.

Confidentiality of communications is one of the most important elements of the protection of the fundamental right to privacy and data protection as well as of secrecy of communications, and any exception to this right and obligation should be limited to what is strictly necessary in a democratic society and clearly defined by law. Blanket retention of all communications data for hypothetical and future criminal investigations would not respect these basic conditions.

"Data retention" requirements would compel agencies accessing and collecting personal information to archive such information for a specified length of time. While many private providers currently retain certain traffic data for billing and other business-related purposes for short periods of time, there are no government-imposed public or private retention requirements in the United States. Wide data retention powers for law enforcement authorities, especially if they are used on a routine basis and on a large part of the population, could have disastrous consequences for the most sensitive and confidential types of personal data. Vast databases now include personal data about medical conditions, racial or ethnic origins, religious or philosophical beliefs, political opinions, trade-union membership, and sexuality. New retention requirements will create new risks to personal privacy, political freedom, freedom of speech, and public safety.

Data retention of communications by law enforcement authorities should only be employed in exceptional cases, and should be authorized only by the competent authorities on a case-by-case basis. When permitted, data retention must be a necessary, appropriate, proportionate and temporary measure. SAR information should be purged from the databases when the statute of limitations of

characterized suspected crimes expires. No SARs should be filed for thresholds below levels where law enforcement will prosecute.

Access to Data

The proposed guidelines and the USA-PATRIOT Act provide additional authorities relating to the collection, use, and dissemination of information sharing of retained data. With such heightened data sharing capabilities, there is an increased likelihood that such information will be misused. In light of this augmented threat to privacy, mechanisms must be established to permit an "audit trail," providing necessary oversight of those granted access to the information. Such a trail was established in the Health Insurance Portability and Accountability Act (HIPAA) guidelines for access to patient data. Specifically, HIPAA provides that an audit log be created of each access [including read-only] to patient data (establishing who accessed which patient's information, what information, and when). Patients are permitted access to this information to ensure that their information is not being misused. A similar audit trail in this context, while not providing such unlimited individual access, would ensure that defendants in criminal trials can evaluate whether their information was improperly accessed or misused by the government. In addition, in order to prevent careless or negligent misuse of information, mechanisms must be put in place providing necessary and adequate training for those granted access to the data.

Foreign intelligence

As the Prosperity Institute Task Force on Information Exchange and Financial Privacy's March 2002 "Report on Financial Privacy, Law Enforcement and Terrorism" explained in greater detail (<http://www.prosperity-institute.org/projects/PI-TF-Report.pdf>), the sharing of information with foreign intelligence will in some cases make us less secure, as some countries' intelligence officials may have terrorist ties. Since some terrorist organizations, according to Attorney General John Ashcroft, use identity fraud to fund their activities, the gathering lots of publicly available information into shared databases creates new dangers.

More people with access to more information on any person present a danger. Authorized personnel, not computer crackers, bring about half or more security problems.

Asset forfeiture abuse

The reach of Section 365 of the USA PATRIOT Act requiring anyone engaging in a trade or business, who receives \$10,000 in a single transaction or two or more related transactions to file a report to FinCEN is too broad. Before authorizing forfeiture of funds due to mistakes made on one of many reporting requirement

forms, an intent to circumvent the law should need to be established. The inclusion of FinCEN Form 8300 in the system for these transactions raises serious questions outlined above.

Respectfully,

J. Bradley Jansen,
Deputy Director,
Center for Technology Policy
Free Congress Foundation

Mikal Condon
Staff Counsel
Electronic Privacy Information Center

Evan Hendricks
Editor
Privacy Times