



**News Release**

**For Immediate Release  
Monday, 9 January 2006**

## **National Biometric Security Project (NBSP) Releases Two Studies on the Impact of Biometrics on U.S. and International Privacy Laws**

### **Studies Highlight Distinction Between Identification and Verification As Key Concept in Applying Privacy Law to Biometrics**

Washington D.C. 9 January 2006 -- The National Biometric Security Project (NBSP) announced the availability of two studies it completed that assess the impact of biometrics on U.S. and international Privacy laws.

***United States Federal Laws Regarding Privacy and Personal Data and Applications to Biometrics*** demonstrates how, under the current U.S. legal system and state of the law at the federal level, use of biometrics as a system to verify identity in virtually any situation is consistent with the law. The report also illustrates how, under certain circumstances, using biometrics to identify individuals through the use of databases is acceptable without sacrificing the objective of maintaining and protecting personal privacy. The report was provided, on request, to the Department of Homeland Security and the Interagency Working Group on Biometrics chaired by the White House Office of Science and Technology.

The report highlights the distinctions in biometric recognition between identification and verification techniques and discusses how each method relates to privacy laws and issues. Generally, biometric "identification" does a "one to many" search of extensive databanks to find a match. Because such databanks may contain or be linked to personal information, and because identification applications can be used without the subject's knowledge or consent, such as in surveillance, the privacy concerns are intensified. Biometric verification systems that use a "one to one" match are generally designed to be used on a voluntary basis. They only require two pieces of information: something representing your identity (such as a user name to retrieve your biometric template or a smart card with your template embedded in it) and your biometric feature or information (such as your hand to create your hand geometry template) presented for the match. Verification systems can be connected to databanks, but unlike identification systems a database is not a necessary component. The need for the subject's consent and the lack of a databank requirement greatly reduce the privacy concerns.

According to John E. Siedlarz, Chairman and CEO of NBSP, "The increasing reliance on biometrics in large scale identification applications such as watch lists, enrollment eligibility and border control applications will require a greater sensitivity to privacy issues to ensure that the rights of individuals are not unduly compromised in the name of security. There are clear steps that can be taken to make all biometric systems 'privacy sensitive'. Those involved in the deployment and management of identification applications will need to employ those steps to maintain the right balance between individual privacy considerations and broader security concerns."

The second study, **Report on International Data Privacy Laws and Application to the Use of Biometrics in the United States**, assesses a broad sampling of international laws that address the subject of privacy and the possible U.S. role in international cooperation in this area. The purpose of this report is to understand international privacy law and its impact on the use of biometric recognition technology on both the United States in isolation and as well as on a global scale.

Resistance to both U.S. and foreign biometric privacy legislation has come from both sides of the fence. Some proponents of biometric recognition technology are concerned that any legislation will restrict the currently legal uses of biometrics. Opponents of biometric recognition technology (on the basis of its perceived threat to privacy) are concerned that legislation will condone the use of such technology on a broad or unrestricted scale. The NBSP concludes that the best compromise is implementation of data privacy policy and/or legislation that takes into consideration: (a) the fact that most overt and consensual uses of biometric recognition technology are legal and non-intrusive; (b) that public concerns over misuses (such as could occur with unauthorized database access or unrestricted data-mining) should be competently addressed; and (c) participation in global privacy standards will enhance proper and effective use of the technology.

This report examines the privacy laws, and in particular the data privacy laws, in the European Union and four other leading industrialized nations and OECD member countries: Canada, Australia, New Zealand, and Japan. In discussing each government, the report includes a brief overview of the legal system, and provides an analysis of the interplay of such privacy laws on local and worldwide use of biometric recognition technology. Also included is a summary of some of the applications of biometric recognition technology in each country and in the EU.

### **About NBSP**

NBSP is a not-for-profit test, research and analysis organization focused entirely on the application of biometrics to improve the security of the U.S. civil infrastructure. NBSP services are available to government agencies at the federal, state, and local level and private sector agencies responsible for maintaining key components of the national infrastructure. The organization can also support non-U.S. nations and organizations involved in the international anti-terrorist coalition when sanctioned by the U.S. government. Established as a non-profit agency to assure its objectivity and user-oriented approach, NBSP client services range from operational/functional requirements definition to standards development, technology/product test and evaluation, research, and data services.

For more information about NBSP please visit us at [www.nationalbiometric.org](http://www.nationalbiometric.org)

For information on acquiring the referenced reports please contact: [ryan@nationalbiometric.org](mailto:ryan@nationalbiometric.org)