

International Conference on Biometrics and Ethics
Ronald Reagan Building
Washington, D.C.

November 28 – 29, 2006

Welcome Remarks

- Bradford J. Wing, Chief Biometrics Engineer, US-VISIT, U.S. Department of Homeland Security (DHS), Chair of Biometrics Coordination Group and John Kropf, Director, International Privacy Policy, Privacy Office, DHS, welcomed the participants. They recognized the theme of the conference, and asked the participants to exchange ideas about biometrics and ethics.

Morning Keynote (Open Media Session)

- Mr. Stewart Baker, Assistant Secretary for Policy, DHS, said uses of biometrics for homeland security became apparent after September 11. He discussed US-VISIT as an example of success. He warned against intentionally placing limitations on who has access to biometrics databases as a privacy safeguard because this prevents necessary and vital information sharing.

Panel 1—Privacy and Ethics under Normal and Extraordinary Circumstances

- The panelists identified issues about social acceptance of biometrics. One panelist pointed out that biometrics change the relationship between individuals and government, because rather than collecting changeable information about a person, such as a name or address, with biometrics, the government collects a permanent and unchangeable part of a person. Errors have much greater implications than in the past.
- Another panelist commented that “biometrics is privacy-neutral,” but that we need to treat biometrics like any other technology system under the Fair Information Principles, primarily with a focus on transparency and redress.
- Participants discussed how to establish a framework that allows the use of biometric data during emergency situations, such as terrorist attacks, epidemics and natural disasters, without violating privacy rights.
- In the conversation that followed the panel, participants discussed the definitions of biometrics and ethics. The conversation about the role of ethics was animated, including how ethics are important to ensure privacy protection during emergency situations where law may be superseded. The participants also discussed the problem of the “permanence” of biometric information and the need for redress mechanisms, and whether it was possible to build privacy policy into the technology itself.

Lunch Keynote

- Mr. Ben Riley, Director of Defense Biometrics, U.S. Department of Defense (DOD), spoke about the uses of biometrics in supporting peacekeeping missions. He discussed the challenges that U.S. forces face in the field. He also referred to many historical texts on peacekeeping operations which recognized the importance of being able to accurately identify members of a population. He explained how DOD

re-structured its research division to focus on biometric technology, and how consideration of privacy implications is part of the DOD's biometrics policy.

Panel 2—Ethics of Biometrics and Health Risks

- During this panel, speakers offered medical and technical reviews of whether fingerprint scanners can transmit infectious diseases. Panelists noted that perceptions of disease transmission may affect the success of a biometric program. Since most biometric enrollments are mandatory, people react to them more negatively than voluntary activities where infectious disease transfer is also possible (e.g., elevator buttons, ATM keypad, bathrooms).
- One panelist encouraged the audience to “anticipate the unanticipated.” He warned that once information is collected for a particular purpose, others will want access that to information for other purposes, and that it is important to know how to deal with such requests in advance.
- In the conversation that followed the panel, participants discussed how public perceptions of biometrics, including issues such as health risks, can affect already implemented programs and create risks to the acceptance of new biometric programs. New technologies may mitigate some risks of disease transfer. Many participants also agreed that biometric users must discuss the ethics of disclosing secondary information revealed during biometric collection.

Day Two

Morning Keynote

- Dr. Emilio Mordini, Director of the Center for Science, Society and Citizenship, University La Sapienza, argued that biometrics is one of the crucial techno-political debates of our era. He reasoned that there is political relevance to establishing someone's identity because a person is ultimately responsible for his or her actions. Following that, human rights and civil liberties can only be protected for known, or “identified” persons. Therefore, it is important to understand how to use biometric technology properly to identify people; it should be done following accepted criteria to ensure that only essential information is collected as needed to establish identity, and that data collected is treated with dignity.

Panel 3—Ethics of International Data Sharing

- The panelists discussed specific examples of how biometric data is shared or can be shared between countries, and what countries are currently doing in those cases to protect privacy. Participants stated many of the benefits of sharing biometric data.
- Participants debated the assertion that the international community has widely divergent views about acceptable levels of data protection.
- The challenge of international data sharing is to share data about persons while respecting dignity, anonymity and other basic privacy rights. One participant asked if a “golden rule” approach would work: Do unto your citizens as we do unto ours. The panelists discussed the differences among countries with regards to recognition of privacy rights, and the importance of agreement on common international privacy principles.

- One participant argued that to define the ethics of biometric data sharing between nations as a choice between human life and human rights is not really a choice, and thus diminishes the ability to engage in real dialogue.

Lunch Keynote (Open Media Session)

- Mr. Robert A. Mocny, Acting Director of US-VISIT, spoke about the value of governments sharing data about criminals and those who would attempt to do harm. He argued that not sharing this data with the appropriate law-enforcement agencies is unethical and that without information sharing, the international community compromises the security of each nation by permitting known criminals to cross borders unimpeded.
- He described the U.S. government's vision of the development of international security standards as one in which governments build an infrastructure that provides a secure environment for information sharing while at the same time protecting privacy.

Panel 4—Government-Industry Collaboration on Biometric Applications

- The final panel examined the relationship between government and industry and collaboration on biometric applications. The panelists shared specific examples of how government and industry work together in symbiotic relationships, but also brought up salient points about the extent to which the government and private industry can intentionally or unintentionally subvert privacy laws in these partnerships.
- Many participants worried that pressures on the government and private industry lead them to collect as much information as they can, and wondered about the ability of entities to enact long-lasting privacy protections. Others saw pressure from the voting public and free market on the government and private industry, respectively, to enact strong privacy protections.

Closing Remarks

- Mr. Maurizio Salvi, Policy Advisor to the President of the European Commission, delivered closing remarks. He spoke about the evolving discussion regarding biometrics and ethics over the years. He also raised the current state of policy decision making in the European Union (EU) and the United States, and asked that participants remember these issues as security will remain a primary policy item in the EU and the United States in the immediate future. He concluded by praising the conference for promoting the principles of open debate, mutual respect, tolerance for other views and public disclosure.