

IDENTITY, SECURITY AND DEMOCRACY

JERUSALEM 2-4 September 2006



POLICY ISSUES AND RECOMMENDATIONS FOR POLICIES

The central question of the meeting was:

**"Should any state, even a democratic State, be entitled with the power to absolutely identify each citizen?
Is such a power ethically tenable in order to secure the common good?"**

CONSENSUS	LESS CONSENSUS OR DISAGREEMENT
<p>Recommendation 1: It is foremost to agree at international level whether, when and to what degree biometrics data are sensitive data.</p> <p>Comment: <i>There are different kinds of biometrics and different applications. We need accepted criteria to be adopted to evaluate the degree of sensitivity of any given set of biometric data.</i></p>	<p>Biometric data as non-irrevocably identifying data are the primary source of security risks to the individual. Only if biometric data are one-way scrambled context-specific in such a way that they can be revoked for this purpose only can we say the sensitivity is reduced. Predictable one-way hashing is not changing the sensitivity level as it creates an easy and non-voluntary identification mechanism (Engberg)</p>
<p>Recommendation 2: Further debate is still required to evaluate the relationship between identification and security.</p> <p>Comment: <i>Policy makers should not assume that "stronger" identification means more effective protection or increased security.</i></p>	<p>For an ethical identity management environment to be achieved, it is important that the public have an understanding of identity management theory, objectives and issues. Without understanding, they will have confused expectations with regard to ethical imperatives. That is particularly so in times when fears of terrorism can be both warranted and manipulated. Secondary schools and universities should include in their curriculum instruction as to rights and obligations relating to identity management and identity theft (Boitel).</p> <p>Identification is both eroding data security and creating a primary risk of identity theft as biometrics is always spoofable (mere constant). In addition non-context specific identification create a source of concentration of power that is a primary threat to democracies. We need to split into the issue of enrolment and non-reputable traceability to a root identity on one side and on top of this the use of context-specific trustworthy (two-way) identity in actual transactions (Engberg).</p>
<p>Recommendation 3: Governments should promote deliberative exercises such as citizens panels and consensus conferences for the purpose of arriving at a consensus as to the balance of appropriate identification inquiry.</p> <p>Comment: <i>It is not clear that all identification should be based on biometrics. Information revealed about an individual should be scalable to the purpose of the inquiry.</i></p>	

<p>Recommendation 4: National governments, international agencies and other public agencies should promote studies and empirical research on: 1) Cultural aspects of privacy; 2) Psycho-social aspects of (perceived) threats to privacy.</p> <p>Comment: <i>The eight principles formulated by the OECD Privacy Guidelines² are critical. Yet they should be considered as a prima facie duty³. Empirical research now is necessary to determine the contextual circumstances in which and extent to which, these principles can be articulated for the purpose of maintaining an appropriate and functional degree of security.</i></p>	<p>Ethical and legal aspects on the right of privacy recognized at international level and laid down in international instruments. (Directive 95/46/EC on data protection) in relation to medical research. Protection of personal data as part of right of privacy The privacy of the individual in the context of the societal interest To reconcile the right of privacy with other interest To find the balance between conflict of interests (individual, societal and other person's) Limits and control of misuse of personal data, liability Regulation of collection, storage, processing and exchange (Tomova).</p>
<p>Recommendation 5: Large scale ID management should be monitored by independent bodies particularly when vulnerable⁴ populations are involved.</p> <p>Comment: <i>In large scale ID management, identification standards and methods should be adopted in accordance with ethical considerations. The respect of fundamental human rights is the presumptive paramount rule.</i></p>	<p>Monitoring does not prevent abuse if abuse due to stripping citizen security through constant identification in transactions is inherent in the design of an Id Management system. To abide to even simple ethical requirement large Scale ID Management system have to enable the use of multiple identities per User. The purpose of root identity systems is not identification but two-way trustworthy security. A typical error in all biometrics is to use foreign readers (ie. Non user controlled on-card match) – such a system cannot be protected and should be last resort after all non-invasive means and technologies have been tested (Engberg).</p>
<p>Recommendation 6: Internationally accepted criteria against which identification procedure can be evaluated whether identification demands are effective and proportionate should be urgently defined .</p> <p>Comment: <i>It is largely accepted that any identification procedure must be proportionate to its intent in order to be ethically acceptable. Yet, there are no established criteria agreed at international level.</i></p>	
<p>Recommendation 7: International initiative to set accepted criteria to safeguard rights of persons without reliable ID (displaced persons, war and disaster, illegal aliens, etc.) should be urgently promoted.</p> <p>Comment: <i>At global level there is an increasing need to provide identification for people without ID. To have an identity is a basic right. However enforcing this right should not become a way to hallmark disadvantaged groups.</i></p>	<p>Serious need to split clearly on the establishment of root identity and identity creation and authentication in use. In case of enrolment of means for the citizen to manage his identities should be included. A biometrics-derived purpose-specific key (i.e. Refugee-specific) can be generated in order to prevent multiple enrolments, but NO storage of non-user controlled biometrics especially not certificates as they are easily abusable for Identity Theft. In case of emergencies without any pre-event preparation an ethical approach should be established according to the type of emergency (Engberg).</p>
<p>Recommendation 8: International governing bodies (OECD, WHO, IOM, World Bank, etc.) should formulate in advance accepted ethical guidance for identity management in emergencies so that it is in place during public emergencies.</p> <p>Comment: <i>We live in a world where emergency is becoming “normal” (terrorism, avian flu, SARS, tsunami, etc.). The exception is becoming the normal condition. Most public emergencies imply the use of intrusive technologies and data management issues.</i></p>	<p>There should be a clear definition of ethics as it applies to identity management.</p> <ol style="list-style-type: none"> What does ethics mean in the IM context? Are there circumstances of national security or personal security under which ethics are irrelevant? How are governmental and private institutions, officials and individuals bound by ethical restraints? When persons have the opportunity to function anonymously should they also be bound by ethical restraints? If so, how? Do ethical obligations go beyond legal obligations? To the extent that ethical obligations go beyond legal obligations, what sanctions should there be for violation of ethical obligations? (Boitel) <p>Means must be developed to ensure that innocent and legitimate citizens can travel and operate without identifying in a cross-context linkable manor. Special consideration needs to be taken to protect the system from becoming a force of power in case of democratic failure (Engberg).</p>

<p>Recommendation 9: Ethical principles should be already defined at system level, so that those who construct the software that manages systems can do so in ways that facilitate and encourage ethical conduct.</p> <p>Comment: <i>The necessary hurdles and hooks must be built into the systems. Retrofitting of such capability may be impossible or very expensive.</i></p>	
<p>Recommendation 10: Funding agencies should promote initiatives in order to set guidelines for the ethical review of research in the field of identification technology and biometrics.</p> <p>Comment: <i>There is a substantial lack of ethical rules for research in the field of biometrics and identification technologies and no initiative is currently in progress.</i></p>	<p>Freedom of research should be foremost (Bromba)</p>

¹ In this context, "stronger" identification means one or more of the following: a) Requirements for an increase in the circumstances or frequency in which identification must be established; b) Higher degree of certainty as to identification – tamperproof credentials, biometrics, state issued credential, biometrics, etc.; c) Mandatory carrying of credentials. d) Record keeping of identification presentation and verification.

² The OECD principles are (OECD, 1980):

Purpose Specification Principle: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Openness Principle: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the Data controller.

Collection Limitation Principle: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle: Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Accountability Principle: A data controller should be accountable for complying with measures which give effect to the principles stated above.

Use Limitation Principle: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle of the OECD Privacy Guidelines except:

- With the consent of the data subject.
- By the authority of law.

Individual Participation Principle: An individual should have the right:

- To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him.
- To have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him.
- To be given reasons if a request made under this principle is denied, and to be able to challenge such denial.
- To challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Security Safeguards Principle: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

³ A prima facie duty is a duty that is binding (obligatory) other things equal, that is, unless it is overridden or trumped by another duty or duties. Another way of putting it is that where there is a prima facie duty to do something, there is at least a fairly strong presumption in favor of doing it.

⁴ "Vulnerable persons are those who are relatively (or absolutely) incapable of protecting their own interests. More formally, they may have insufficient power, intelligence, education, resources, strength, or other needed attributes to protect their own interests" (CIOMS International Ethical Guidelines for Biomedical Research Involving Human Subject, 2002). WHO and CIOMS ethical guidelines specifies certain vulnerable categories (children, prisoners, pregnant women, and persons who are handicapped, mentally disabled, economically disadvantaged, or educationally disadvantaged). However the guidelines are not intended to be exclusive, leaving open the interpretation of vulnerability.