Number	LANCS-D4.1-RN-D-Flagship.1	A-PI--

Title	Research Note (RN) for D4.1
Subtitle	Ethical aspects of development **D : Flagship Development** : *Biometric Identification*

PROBLEM		SOLUTION	

Research Note	X	Selected Annotation	

Categories: | | |

Summary:

This note addresses the use of biometric identification and takes particular issue with the ethics of governance and ethics of decision-making in relation to the use of biometrics.

CONTEXT

Europe has followed a global trend towards securitization to justify the use of advanced ICTs to protect freedoms and combat cross-border crime, fraud and terrorist activities. Particular emphasis has been on the use of biometrics for identification, a shared visa system and other border controls.

(Key readings include, Alterman, 2003; Amoore, 2006; Balzacq and Carrera, 2006; Raab and Bennettt, 1994; Bigo and Guild, 2005; Bigo and Tsoukala, 2006; Bigo et al, 2007; Cooper, 2010; Council of the European Communities, 2000; Council of the European Union, 2008; De Hert, 2008; European Commission, 2008; European Parliament legislative resolution, 2009; Hayes, 2006; HIDE, 2008; Hornung et al, 2010; Joint Research Center, 2005; Kevenaar et al, 2010; Liberatore, 2007; Lodge, 2006; Lodge, 2007b; Lyon, 2003; Mordini and Massari, 2008; Rahmun and Hick, 2010; van der Ploeg, 1999; Yannopoulos et al, 2008)

FACTS

The honesty with which the potentials and limitations of biometric systems are communicated is either lacking or, worse, the limitations are only discovered too late. For example, including biometrics in large scale databases for ID card or passport registries, visa enrolment, and other record keeping, is technically and operationally problematic. There are multiple interaction nodes along the trajectory of enrolling the data, creating biometric templates and random number encryptions, storing and processing them, and providing access across jurisdictions. Each point of interaction is vulnerable to illegitimate insertion, extraction, alteration or deletion of data (e.g. Kevenaar et al, 2010). But solutions to these problems of reliability and dependability do not seem to have the highest priority and the policy goals risk being incompatible with realistic expectations of both the capabilities and the vulnerabilities (see Lodge, 2007 on this issue).

COMMENT

Questioning the assumptions on which 'security' already rests, opens the door to alternative ways of framing what the problems might be and, consequently, which issues need discussing and debating. The vast distribution of ICTs for surveillance and security purposes, including the uses of biometrics, legitimises the involvement of publics beyond the official institutional protocols for public engagement. The doors could be opened to alternative views which already are struggling to find legitimacy using the conventional public engagement methods. According to a recent FP7-funded research project, Technolife, public assumptions about the uses of biometrics are very diverse:

1. Biometric and other information technologies are necessary, bound to occur because governments must be allowed to identify those who are a threat to ensure the continued safety and well-being of citizens.
    - Uncertainties are primarily about who people are, the risks associated with letting them roam freely, the danger that someone wants to harm 'us'. The means of control are to track individuals and collect information, including biometrics.
2. Biometric technologies are positive, interesting and good to have but the stated certainties and uncertainties about them are subject to doubt. Asking critical questions opens up avenues for further enquiries about necessary personal control over privacy, whether the technology is safe, how it can be abused or to what extent the technology still needs figuring out. The law may not be adequately addressed either, nor the EU objective of social inclusion.
    - Uncertainties are related to safety, decision-making and operation. The risks are associated with potential identity theft and unfair exclusion. The danger is that potential problems and uses are not debated, and control is associated with the power to include and exclude, to control private information or someone else's identity.
3. Conventional depictions of the world we live in (including the need for biometrics for human security) are utterly mistaken because they do not adequately question computing systems, governance or the social and ethical costs we already pay in Western democracies for an obsolete socio-economic and political system.
    - Typical questions of uncertainty, risk, danger and control never get at the 'bigger', the 'right' and the 'real' questions of what the world needs, what people actually want, why technology is made central, what meanings are attached to safety, a good life, and so on.

What the third example here shows is how ethical reflection can be a tool to reframe completely what the key problems are and which issues need discussion and debate – where publics find an outlet for political and socio-economic dispositions which have considerable currency but appear to be ideological 'no-go-zones' in conventional democratic deliberation. For example, the sanity of the securitization trend could be made subject to considerable doubt. The question is raised if Western democracies emphasise the use biometrics to secure themselves from so-called enemies of democracy, whose grievances are merely the symptoms of 'us' imposing on 'them' oppressive non-democratic socio-economic regimes to support global capitalist and militarist agendas which are essentially indefensible and unsustainable. Paradoxically, publics also appear to seek an outlet to express sentiments that strongly signal a cultivation of social paranoia in the current political climate, of grappling with citizenship, transnational development and securitization. However, most of these dispositions, and the ways in which they reframe problems and debates, are likely to be ignored or played down in the foreseeable future.