SEVENTH FRAMEWORK PROGRAMME
Capacities Work Programme: Part 5 – Science in Society

Call: FP7-SCIENCE IN-SOCIETY-2008-1

Topic: SiS-2008-1.1.2.1 Ethics and new and emerging fields of science and technology

Project acronym: TECHNOLIFE
Project full title: a Transdisciplinary approach to the Emerging CHallenges of NOvel technologies: Lifeworld and Imaginaries in Foresight and Ethics

Grant agreement no.: 230381

Deliverable 5.2…

Report: ICT research line – main results and policy recommendations:

Biometrics and mobility in the EU: point of view of deliberation

Authors: Kjetil Rommetveit, Kristrun Gunnarsdóttir, Adrian MacKenzie, Brian Wynne, Margit Sutrop, Roger Strand

This report, with dissemination restricted to EC use, builds upon previous deliverables of the TECHNOLIFE project and also contains overlapping sections with and excerpts from D1.1, D4, D4.1, and D5.1.1

Introduction to the TECHNOLIFE method

The TECHNOLIFE project is a methodological and conceptual research project designed to provide ethical frameworks for new and emerging sciences and technologies. One of the technological fields investigated by TECHNOLIFE is biometrics. This report briefly explains the method and the results, and provides our policy recommendations to the European Commission.

The TECHNOLIFE method maps ethical issues at early stages of S&T and policy development and represents social imaginaries relating to these ethical issues.

This method is a suite of exploratory, qualitative and quantitative approaches and consists of the following steps:

1. An ethical issues scoping exercise that defines **hot topics** in relation to the technological fields. Hot topics are issues of concern that involve unsolved social, moral and/or political tensions and that are immature for regulatory definition and resolution. In the definition of hot topics, emphasis is placed on situating them with reference to pre-existing cultural understandings and imaginations.
2. A **participatory, deliberative exercise** in which groups of citizens and stakeholders discuss the hot topics. The purpose of the exercise is to elicit arguments, concerns, imaginaries and alternative frames of understanding with respect to central policy issues seen in the light of broader cultural developments. To this end, a protocol has been developed. The protocol includes principles for the selection and recruitment of groups; the construction of media objects (especially films) in conjunction with social media; an online forum tool that is part of the specially designed **KerTechno** software. KerTechno is a tailored, open-source, web-based deliberative software solution building upon the previous KerBabel deliberative software and specifically developed for TECHNOLIFE; as well as principles for moderation of the deliberation.
3. An online **voting system** for deliberative purposes that is integrated in the KerTechno software and that allows for **quantitative analysis** of results.
4. A qualitative, **analytical procedure** that identifies the arguments, concerns, imaginaries and alternative frames of understanding elicited by the participatory exercise and defines their relation and relevance to early stages of S&T and policy development.

Structure of the report:

Introduction: biometrics as a technology of governance

Narrowly defined biometrics is the application of scientific measurements to the human body. Biometrics is a tool used to identify and confirm an individual´s identity on the basis of physiological or behavioural characteristics (or a combination of both), which are unique for a specific human being[1]. Such characteristics are facial image, fingerprints, hand geometry, the structure of the retina or iris, DNA, gait, heart pulse, voice and others. Biometric are increasingly embedded within large-scale information structures and operating across physical/digital interfaces through sensors such as biometrics readers and imaging technologies for uses in large crowds (mostly driven by emerging pattern recognition software and algorithms designed to extract unique physical features from individual bodies). Biometrics´ purpose is not to understand bodies, but rather to use their features to identify individuals or even to predict people's behaviour or intentions (to identify suspect behaviour or hostile intents) as they cross borders, move in public spaces, use critical infrastructure, reside on territories, make transactions and interact with societal institutions (to mention some of the most central uses). James Scott describes how a certain *state vision* has been endemic to the increasingly specialised and expert-dominated planning and organisation of modern societies. It is targeted and purpose-directed, constructing and projecting a kind of map "designed to summarize precisely those aspects of a complex world that are of immediate interest to the map-maker and to ignore the rest" [2]. Biometrics is literally a technology that provides what Scott terms "eligibility": it renders subjects and citizens visible to the state, hence also (potentially) controllable[3]. Biometrics is very much a *social technology*, not directed at something "out there" (like quarks or DNA), but at basic human relations such as trust and dis-trust among different groups, security and insecurity of human relations and transactions. It is, of course, also deeply inscribed with many of the industrial and monetary values that go to make up global flows of capital, people and information.

As we speak, biometric information systems are being implemented throughout the European member states, in many cases as a direct result of a concerted European policy. This is especially so for biometric passports and travel documents (visa and residence permits), as implemented in the visa system (VIS) and in the implementation of the second generation of the Schengen Information System (SIS II). The Eurodac automatic fingerprint system (AFIS) has already been in use since 2003 for registration and monitoring of asylum seekers and "illegal immigrants". In an increasing number of countries, such initiatives have come to go hand in hand with national databases and information systems, as well as the introduction of other types of biometric tokens, such as national identity cards and driver´s licences [4].

Taking account of the Technolife methodology and conceptual approach, the exposition will be as follows: first, a description of a *socio-technical imaginary* (Jasanoff and Kim 2009), that guides the implementation of biometrics, and as such is a concretisation. This imaginary should be seen as a response to challenges posed by securitisation. Second, we provide a critical analysis of securitisation and the central policy metaphor set to regulate the biometric field of emergence/emergency. This is the "balance metaphor", stating the possibility and necessity to "balance privacy with security", or "freedom with security". Third, since Technolife is a participatory project, we reflect on the wider conditions of possibility for undertaking such an exercise on a European level. Fourth, drawing upon results from the Technolife forum, we analyse modes of reasoning and deliberating about biometrics, including a set of alternative imaginaries of biometrics and society. Fifth, we sum up the analysis with a set of concrete policy recommendations.

---

[1] Future of Identity in the Information Society (FIDIS). (2009). D3.10: Biometrics in identity management.

[2] Scott, JC (1998) *Seeing Like a State. How Certain Schemes to Improve the Human Condition Have Failed.* New Haven and London: Yale University Press, p. 87.

[3] Lyon D (2009) *Identifying Citizens. ID Cards as Surveillance.* Cambridge, UK: Polity Press.

[4] Bennet C. J. and Lyon, D. (Eds.) (2008) *Playing the Identity Card. Surveillance, Security and Identification in Global Perspective.* London and New York: Routledge.

1. The biometric imaginary

Shortly after 9/11 a great number of initiatives and new legislation were made by the US Congress to heighten security measures across a number of fields. The notion soon took hold that there is a strong connection between travel documents, the fight against terrorism and biometrics. The implications of the 9/11 Commission´s statement that "for terrorists, travel documents are as important as weapons" [5], says something about the expanding scope of security in those days: extremely few people are terrorists, but almost everybody hold travel documents of one kind or other. The biometrics industry and lobby moved fast to ensure its place within this enlarged space of opportunity. The US Congress dealt with a great number of proposals for new legislation entailing biometrics and other security technologies [6]. One main outcome of the hectic legislative activity was the *US Patriot Act*. The *Department of Homeland Security* was set up to deal with terrorist threats and a *National Strategy for Homeland Security* was issued by the Bush administration. The ensuing *U.S. VISIT* programme require the taking of fingerprints and facial scans of all foreign nationals entering or exiting the United States, to be checked against databases and watch lists such as the *Terrorist Screening Database* and the AFIS system of the FBI [7]. By 2004 the Department of Homeland Security was demanding that all countries in the Visa Waiver[8] programme should implement biometrics in passports and travel documents by a set date (26 October 2004, but the deadline was later prolonged by two years). Countries that did not comply would be ousted from the programme.

The "basic dogma of biometrics states that "*An individual is more likely similar to him- or herself over time than to anyone else likely to be encountered"* [9]. As such, this premise is not much different from those made in fingerprinting or in long-standing biomedical traditions viewing bodily information, such as proteins, blood type and DNA, as highly specific, and so usable for identification purposes. However, a second, highly powerful premise was also introduced. This came along with the increasing potential for digitalisation of such information, and for the exchange of information between operators, i.e. *systems interoperability*. The US National Security Strategy stated that *"…government agencies storing terrorism information, such as terrorist "watch lists," have not been able to systematically share that information with other agencies. These differences can sometimes result in errors if, for example, visa applications and border controls are not checked against consistent "watch lists"* [10]. The document outlines a "system of systems" to deal with the integration of sources of information. As in many documents promoting interoperability, two elements are highlighted as crucial: first, information systems must be made to communicate. Second, legal, organizational and cultural barriers must be removed so that information can be exchanged freely and used effectively. The implication is that biometric information may serve as a better medium for the connection of previously un-connected sources of information (mainly databases), and that this will turn out beneficial in operational and organisational terms. Finally, under conditions of high political urgency, but also helped by strong pressures by industry, the fundamental dogma and the interoperability thesis have been implemented into something approaching a global vision for mobility, security and border management. A succinct statement of this border management regime

---

[5] National Commission on Terrorist Attacks upon the United States (2004) The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States. http://www.9-11commission.gov/report/index.htm, p. 384.

[6] Zureik E and Hindle, K. (2004). Governance, security and technology: The case of biometrics. *Studies in Political Economy*, 73, 113-137.

[7] Aus, J. P. (2006) 'Eurodac: A Solution Looking for a Problem?'. *ARENA Working Paper No. 09*. (Oslo: ARENA. Centre for European Studies, University of Oslo).

[8] Citizens of countries included in the US Visa Waiver program can travel to the US for up to 90 days without a visa.

[9] National Research Council 2011

[10] US Office of Homeland Security (2002) US National Security Strategy. http://www.au.af.mil/au/awc/awcgate/nss/nss_sep2002.pdf

was made by then secretary of Homeland Security, Michael Chertoff, while speaking of US – EU relations in Berlin, 2005:

"Allow me to share with you where I would like to see us move - toward a world that is banded together by security envelopes, meaning secure environments through which people and cargo can move rapidly, efficiently, and safely without sacrificing security or privacy…For those within the security envelope, we will have a high degree of confidence and trust, so that trusted travellers and shippers don't have to be stopped at every point along the way to be re-vetted and rechecked. And that would enable us to focus more of our resources for those outside the security envelope - for the kind of in-depth analysis and the kind of in-depth vetting that is necessary to make sure those who seek to harm us do not slip through the cracks".

The biometrics imaginary was exported mainly through two international organisations: the G8 and the International Civil Aviation Organisation (ICAO). The G8 provided a forum in which the leaders of the industrialised world agreed to introduce the technology; the ICAO worked out technical specifications in order to promote standardisation and interoperability on a global scale. The 2002 Berlin Resolution of the ICAO decided on the *face* as the globally interoperable standard for passports and travel documents. Following this, the main document has become the ICAO *Doc. No 9303*, making the facial image the primary and mandatory biometric, with fingerprints and iris scans as optional alternatives.

1.1. Introducing biometrics in the EU

The biometric transforming imaginary easily lent itself to political visions of enhanced border control as a way of promoting European integration. The relevance of 9/11 for increased use of biometrics was openly recognised by EU policy makers: *"In the aftermath of the tragic events of September 11, 2001 the Commission was asked by Member States to take immediate action in order to improve document safety"* [11]. Notably, the "Member States" in question were mainly those taking part in the G8: England, Germany, France and Italy (also joined by Spain). From the outset, a unified and overarching approach was pursued. The 2003 Council of Thessaloniki stated that: *"…a coherent approach is needed in the EU on biometric identifiers or biometric data, which would result in harmonised solutions for documents for third country nationals, EU citizens' passports and information systems (VIS and SIS II). The European Council invites the Commission to prepare the appropriate proposals, starting with visas, while fully respecting the envisaged timetable for the introduction of the Schengen Information System II"* [12]. This constitutes the EU parallel to (and continuation of) the US biometrics vision. But it also marks a new stage in the project of European integration and the wider contexts of that process. This was not only so because of strong calls for tighter security measures in controlling the common external border; it also came along with the expansion of the EU towards 10 new member states in 2004. Ensuing legislative initiatives issued in two coordinated, still separate, batches of legislative initiatives. Important to both is the occurrence of a "policy vacuum" following 9/11, and the ways in which this opened up an enlarged space of opportunity for biometrics.

1.1.2. Biometrics in travel documents.

In September 2001 the European Commission submitted proposals to the Parliament and Council for enhancements of security standards in visas and residence permits for third country nationals, both of which were adopted in February the following year. Neither proposal included biometrics. Following

[11] European Commission (2003) Proposal for a COUNCIL REGULATION amending Regulation (EC) 1683/95 laying down a uniform format for visas. Proposal for a COUNCIL REGULATION amending Regulation (EC) 1030/2002 laying down a uniform format for residence permits for third-country nationals. COM/2003/558 final.

[12] European Council (2003) Presidency Conclusions – Thessaloniki, 19 and 20 June 2003. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/76279.pdf

the Councils of Laeken, Sevilla and Thessaloniki, however, the proposals for visas and residence permits were again amended, this time with the twin aims of bringing forward the implementation of security standards (from 2007 to 2005), and to introduce biometric identifiers. In September 2003 the Commission issued another proposal for amending the regulations of visas and residence permits[13]. This time facial photography was included as the primary biometric identifier and fingerprints as secondary. Both were obligatory and both were to be implemented on the medium of a contactless chip [14].

Following this, and using the same technical committee as for visas and residence permits, parallel proposals were developed for biometrics in European citizens' passports. In February 2004 the Commission presented a proposal, the main rationale of which was to "establish a reliable link between the genuine holder and the document" and so to "fight the use of false documents" (European Commission 2004). The Council decision was far from unanimous and came out of a private meeting of the "G5"[15] in Florence, Italy[16], hence by-passing ordinary decision making procedures in the Council[17].

The process of introducing biometrics into travellers' documents in the European Union came as the result of concerted processes in high political circles. Decisions were not made without opposition, but criticism never ventured far outside elite levels, such as ministers from smaller countries in the Council, privacy commissioners and privacy advocates. The European Parliament arranged for a hearing, including technical and legal expertise. The ensuing report criticised the lack of democratic control and the mis-match between political and technical decision making: *"It should be emphasised that the European Council made a political decision to introduce biometric identifiers in EU passports without any input from practitioners and without knowing the magnitude of the problem"* [18].

1.1.3. Interoperable information systems.

As required by the Council at Thessaloniki, the biometrics strategy was seen in conjunction with the establishment of a number of large-scale biometric information systems [19]. The example *par excellence* of such a system would be the SIS and its transformation into SIS II[20]. From the outset, the purpose of SIS ("the backbone of Schengen") was to "maintain public order and safety" (CIS Art 93) by fortifying controls and security at the external Schengen border as the internal borders were abolished [21]. The system contains alerts on people (and property) to be extradited, denied entry, placed under surveillance or interrogated. The impetus for expanding the original system, operative since 1995, was not to fight terrorism, but came as a natural result of the expansion of the EU. The need for technological upgrades was also important, but biometrics was not mentioned. Two years later, this

[13] European Commission 2003

[14] Due to technical problems with the visa stickers, the proposal was not implemented into law until 2006. The choice of contactless chips entailed the use of RFIDs, thus settling for a more complicated option than that chosen in the US. The inclusion of RFIDs in travel documents and passports has been a source of much criticism, not the least due to increased risks of spoofing (i.e. hacking into documents from a distance).

[15] The 4 European G8 member states + Spain

[16] La Republica. (18 October 2004). Impronte sui passaporti nella UE.

[17] Aus 2006

[18] LIBE (2004) 'Report on the Commission proposal for a Council regulation amending Regulation (EC) No 1683/95 laying down a uniform format for visas and the Commission Proposal for a Council regulation amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals, (Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Carlos Coelho).

[19] A number of other databases, not dealt with in this article, are also being developed. VIS SIS II and Eurodac are among the biggest and most important.

[20] Denoting, respectively, the first and second generation of the Schengen Information System. The plan was for transition from SIS to SIS II in 2007, but rollout has been delayed due to a number of problems.

[21] Some of the rationale of this is further described by Gunnarsdottir, this edition.

had changed: *"the system should provide the flexibility to incorporate new functionalities, as well as new information and rules without major technical changes. This would include the inter-linking of alerts and the use of biometric information"* [22]. Another important concept had also found its way into the document, that of *interoperability*. On a conspicuous level, this entailed the requirement that the member states implemented compatible (or "harmonised") standards for the exchange of biometric data within the SIS II itself. But it also came along with the further requirement that *"The compatibility with other relevant - existing or future - databases in these fields is of the utmost importance"* [23]. This entails that the central system, to the greatest possible extent, be made interoperable with existing *national* systems (especially automated fingerprint identification systems, AFIS). But it also meant that the SIS II be made to exploit potential synergies with other European systems, especially VIS, but also with the EURODAC system and others [24].

Whereas the SIS II had been planned since the 1990s, the Visa Information System was a genuine child of the situation in the early 2000s. The idea of a centralised system for the collection and exchange of visa data was put forth by the German government in the direct aftermath of 9/11 [25]. A Commission feasibility study estimated that the system would connect the visa authorities of 27 countries, 12 000 operators and 3500 consular posts worldwide[26]. The system was anticipated to process approximately 20 million applications each year. The data would be stored for five years, resulting in a number of approximately 70 million datasets at any given time. Awaiting the possible implementation of the European Passport Registry and the SIS II, this would make the VIS the largest biometric database in the world. The system will share a "common technical platform" with SIS II. It consists of a centralised base, C-VIS, operating and coordinating the system of national contact points, called N-VIS, and these will be connected to local contact points, such as consulates or immigration offices. The systems would also share the Biometric Matching System (BMS), required for reading and comparing biometric data.

The two systems should have separate legal bases, and their uses kept separate, in the sense that data stored on SIS II should not be matched with data stored on VIS (or EURODAC, or any other system). The main users of SIS II would be police, border guards, internal security and immigration authorities; for VIS it would be consular posts, border guards and immigration authorities. Cross-uses were imagined, for instance by giving consular posts access to SIS II data as part of visa procedures or internal security access to visa or immigration data. Consular and immigration authorities already have access to the SIS, and they will be given continued access to the SIS II. What was new was access for police, security and judicial authorities to the VIS. For such access to be granted, extraordinary circumstances would have to apply, i.e. "overriding public security concern"[27]. But in spite of such precautions the purposes of the systems are expanded. The SIS II is no longer restricted to "security checks" (as with the SIS) but has become a system for "prevention, detection or investigation", potentially including alerts on "persons who are likely to commit serious offences"[28]. The interlinking of alerts has the potential of creating new kinds of information on individuals (such as profiles). Similar things go for the promise to use biometrics and not alphanumerics for database searches (a facial image or fingerprint may generate much larger amounts of matches from a radically expanded set of sources). Finally, the number of agencies to be granted access has expanded, and the purposes of the systems are defined in looser terms, not the least in order to remain "flexible".

In the 2005 Hague program the described developments were included within an "integrated management" of the external borders (initiated at the Laeken Council in 2002). Following the Hague

---

[22] European Commission (2003b) COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT. Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS). COM/2003/0771 final.

[23] *ibid.*

[24] European Commission (2005) 'Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597', in European Commission.

[25] Aus 2006

[26] European Commission 2003b

[27] European Commission 2005

[28] *ibid.*

program the Integrated Border Management Strategy has been fortified and now makes up the most comprehensive framework for understanding and implementing biometrics for migration control in the Schengen area[29]. Through interoperable biometric systems the border is imagined as fortified and enhanced in at least two respects. First, the border itself is enhanced through increased capacities of border guards for "seeing" and controlling individuals at the same time as throughput is enhanced, especially through automation: *"One border guard should be able to oversee up to ten automated border gates in operation. Automated border controls for bona fide travellers would provide major benefits in time savings on crossing the external border and allow border authorities to focus their resources on those groups of third country nationals that require more attention, thus improving overall security at borders"* (*ibid.*). Second, the border itself is expanded in time and space, even to the extent that "the border is everywhere" (Lyon 2005). The new management strategy entails "measures taken at the consulates of third countries, measures at the border itself and measures inside the Schengen area" (Commission 2008). At consulates, visa applicants will be subject to a more thorough pre-screening process, by being checked against VIS and SIS II. Awaiting the rollout of VIS (from 2009 onwards) an entry-exit database was also envisioned that could keep track of visa over-stayers (by far accounting for the greatest amount of "illegal immigrants" in the EU).

2.1. Policy context 1: Balancing freedom and security?

As remarked, biometrics enters into extremely complex fields of diverging, though increasingly also interrelated processes. Sovereign territories, policies and populations are seeking closer collaborations while at the same time responding to new security challenges. Asylum, foreign relations, judicial cooperation and customs controls: these are examples of domains that traditionally would exist as separate, although on occasion they would also happen to intersect. In the European Union, the establishment of a distinct policy domain, the Area of Freedom, Security and Justice, along with the changing security landscape after the fall of the Berlin Wall and the World Trade Centre, seems to pull such domains into tighter interconnectedness. Biometrics has come to occupy a prominent position within these reconfigurations. Following authors such as Angela Liberatore[30] and Didier Bigo[31], the unfolding of biometric systems and the wider Area of Freedom, Security and Justice, may be grasped as taking shape through an unfolding imaginary of *securitisation*. By "securitisation" we imply processes by which an increasing number of issues are imagined and framed in terms of security concerns, organisational measures and technologies. As just stated, these are also processes through which a number of boundaries are redrawn, between policies and different territorial borders. Clearly, these are also social and ethical boundaries, the fundamental issue being the delineation between groups and their corresponding rights, such as EU citizens, *bona fide* travellers or "illegal immigrants". The discourse of securitisation may be observed to take place on a number of levels:

-*politically,* through a general drift in the priorities set by the European Council, especially during the early years of introducing biometrics in the EU. Thierry Balzacq and Sergio Carrera, in observing the guiding values of the Tampere (1999) and the Hague (2004) programmes, comment that:

"In fact, the 'shared commitment to freedom based on human rights, democratic institutions and the rule of law' as set out at Tampere, is not a cornerstone of its successor. The Council now gives a high priority to security, meaning 'the development of an area of freedom, security and justice, responding to a central concern of the peoples of the States brought together in the Union'. 'The central concern of people of the States' is thus translated into a security-led approach which dominates the Programme"[32]

[29] European Commission 2008
[30] Liberatore 2006
[31] Bigo 2000, 2006.
[32] Balzacq and Carrera 2006, 5.

Biometrics enters nicely into this image of a revised, overall policy architecture. The main body of text of the Hague Programme, called "Specific orientations", is divided into three comprehensive sections, "Strengthening freedom", "Strengthening security" and "Strengthening justice". One may indeed wonder why the paragraph dealing with "Biometrics and information systems" (1.7.2), has been placed under the general section on freedom, and not that of security. Says Didier Bigo: "…the second section on security has infiltrated and contaminated the other two on freedom and justice"[33].

As noted by Bigo, Liberatore and others[34], contestations as well as promotion of securitisation tend to revolve around different views and uses of one central metaphor: that of *striking the right balance* between freedom and security. The policy literature abounds with expressions such as: *It is…important not to lose sight of the need for a proper balance between the reinforcement of security and due regard for the individual rights of the persons concerned*[35]*; the Union needs to strike the right balance between privacy and security in sharing information among law enforcement and judicial authorities*[36]*; It is part of the balanced Commission approach to take into account possible negative effects on human rights, notably privacy rights of citizen*[37]. From such over-arching declarations and programmatic statements in central documents and speeches, the metaphor stretches deep into concrete processes and negotiations shaping institutions, legal frameworks and technologies:

-*the legislative process* can be seen as an ongoing struggle by privacy authorities and advocates to contain tendencies towards extended authority and access for Europol, internal security and other agencies within the limits set by privacy regulations. The European Data Protection Directive is the central touching stone here. Article 6 (b) of the directive states that data can only be processed for specified and explicit purposes, 6(c) that such processing must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed.

For instance: In the opinion of the European Data Protection Supervisor the proposal for regulation of a second generation Schengen Information System entailed an undue expansion of the systems objective in comparison to the previous system (SIS):

"The objective of the SIS II seems much broader than the objective of the current SIS as laid down in Article 92 of the Schengen Convention, which referred specifically to '(...) access alerts on persons and property for the purposes of border checks and other police and customs checks'"[38].

---

[33] Didier Bigo, *Liberty, whose Liberty? The Hague Programme and the Conception of Freedom*. In Thierry Balzacq and Sergio Carrera (eds.) Security versus Freedom? A Challenge for Europe's Future, Ashgate 2006.

[34] See for instance Lyon, D. (2003) *Surveillance after September 11* (Cambridge: Polity Press); Amoore, L. (2009) 'Algorithmic War: Everyday Geographies of the War on Terror', *Antipode* 41/ 1: 49-69; Huysmans, J. (2006) *The Politics of Insecurity. Fear, migration and asylum in the EU* (London and New York: Routledge); Muller, B. (2008) 'Travelers, Borders, Dangers: Locating the Political at the Biometric Border', in M. Salter (ed), *Politics at the Airport* (Minneapolis and London: University of Minnesota Press); Epstein, C. (2007) 'Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders', *International Political Sociology* 1: 149-64.

[35] 2004/0039 (CNS)

[36] The Hague Programme: Ten priorities for the next five years A partnership for European renewal

[37] Hobbing 2006

[38] European Data Protection Supervisor (2006): Opinion of the European Data Protection Supervisor — on the Proposal for a Council Decision on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)230 final); — the Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II) (COM(2005)236 final), and — the Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates (COM(2005) 237 final)

However: In the final Regulation the general purpose of the system seemed to have been, if anything, further expanded. Article 1.2 now reads:

"The purpose of SIS II shall be, in accordance with this Regulation, to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States, and to apply the provisions of Title IV of Part Three of the Treaty relating to the movement of persons in their territories, using information communicated via this system"[39].

Hence, in this context, "balancing" implies expanded rights of access to those instigated to maintain public security and public policy. Hence, "balancing" is predicated on the expansion of securitisation.

-*technically*: On a technical level a number of political decisions are made, and many of these are also framed in terms of security versus privacy. For instance, the new biometric passport uses a so-called "contact-less chip" (Radio Frequency Chip, RFC) as storage medium for the biometric data. This entails that every passport can be read at a distance, from about 10 feet away[40]. One problem with this is that it opens up the possibility of "spoofing", where un-authorised third persons hack into one's passport and download the data contained, for instance using a portable reader. The alternative to this solution would have been a contact chip, requiring the passport holder to physically interact with the reader, and so the biometric data cannot be read from a distance[41]. As towards this seemingly more privacy-friendly solution, the EU passport now comes with another "privacy-enhancing technology", so-called extended access control, meant to deal with the problem[42].

An even more telling example would be the calibration of the systems themselves. A biometric system will never be flawless, which follows from the changeable character of its object: the human body. The body changes, and so may not be the same at the time of control as upon enrolment into the system. The technical literature[43] distinguishes between two main types of error[44]: the first is *false acceptance* (false match) in which an individual is erroneously accepted by the system (i.e. person X is not who he claims to be). The second is *false rejection* (false non-match), entailing a failure to match the individual with the biometric data registered by the system (i.e. person Y is who she claims to be but is not recognised by the system and so rejected). These parameters are internally related: calibrating the system towards reduction of the number of false matches will cause the number of false rejections to go up[45]. Thus, the different parameters come to be displayed as trade-offs involving political and ethical choices, in which concerns related to security, privacy and efficiency are (allegedly) *balanced* against each other.

From such examples it may be inferred that the balancing metaphor covers many aspects important to the regulation of biometrics. However, to forestall one of the main recommendations of this report: whereas the balancing metaphor may be useful in certain well-defined and concrete contexts, as an over-arching approach it may be elusive. This is first and foremost so due to the experimental character of the biometric systems dealt with in this report: applications at the scale at which we are

---

[39] Regulation (EC) No 1987/2006 of 20 December 2006 of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS II).

[40] Hoepman et al (2006): *Crossing Borders: Security and Privacy Issues of the European e-Passport*. The assessment is based on involvements with the Dutch implementation of the e-passport, on technical tests of the passport and access to confidential EU policy documents.

[41] De Hert and Sprokkereef 2006.

[42] Hoepman et al. 2006

[43] See for instance the 2005 JRC Report *Biometrics at the Frontier*.

[44] Analogous to Type 1 and Type 2 errors in scientific experiments.

[45] Face Recognition Vendor Test 2002.

talking, i.e. Europe-wide, have never been carried out and tested in practice. Indeed, the immature character of the technology bespeaks the high level of urgency with which it has been ushered in. This was underlined in the 2004 report for the European Parliament[46], and it has been emphasised by a number of researchers involved in the development of biometrics:

"The effectiveness of biometry is highly overrated, especially by politicians and policy makers. Despite rapid growth in applications, the large-scale use of biometry is untested. The difficulty is that it is not only unproven in a huge single application (such as e-passports), but also not with many different applications in parallel (including "biometry for fun"). The interference caused by the diversity of applications—each with its own security policy, if any—may lead to unforeseen forms of fraud" [47].

If this is right, it seems to follow that we do not really know what constitutes "security" in our balancing equation. A further issue, to be dealt with in more detail in the next section, strengthens this: the organizational and cultural difficulties in getting the members of 27 different nationalities to stabilize action and collaboration around a set of categories and commands (i.e. "hits" in the system), are immense. This goes some way in questioning the other side of the balancing equation, namely "privacy". How do we know how to define and make operational privacy within such large information structures? How do we know whether it has been strengthened or weakened? According to the literature privacy is a "subjective value", in need of articulation by concerned subjects situated within concrete contexts [48]. This also points to what we shall have to say in the next section, dealing more with the deliberative aspects of policy making. For how, if concerned parties do not discuss the technology, may we know what constitutes "privacy" in biometric systems?[49]

2.2. Policy context 2: Conditions of debate

The concerted pushing of the biometric "security envelope" (see page …) on high political levels structures the kinds of policy responses, including those from the wider publics, to be considered as the technology becomes implemented. Public debates have taken place within national contexts, especially the debate over national ID cards in the UK[50]. As for biometrics in visas, residence permits and passports, however, developments have been pushed through at the highest of political levels, giving rise to concerns that a kind of "policy laundering"[51] is taking place: the European members of the G8 (Germany, UK, France and Italy), acting under pressure from the US, may have used the European Council to promote national security interests, thereby by-passing national parliaments. This, combined with high levels of secrecy and tight relations between industry and government actors, has had negative consequences for the conditions of public debate. This is important for the conditions of carrying out a meaningful debate, such as that undertaken by Technolife. We therefore describe in some more detail how

[46] LIBE 2004

[47] Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur, "Crossing Borders: Security and Privacy Issues of the European e-Passport", In *Yoshiura*, Hiroshi (*ed.*) et *al.*, Advances in information and computer security. First international workshop on security, *IWSEC 2006*, Kyoto, Japan, October 23-24.

[48] Solove, D.J. Understanding Privacy, Harvard University Press, Boston, 2008.

[49] Rommetveit, K. 2011. "Tackling epistemological naivety: large-scale information systems and the complexities of the common good", special issue Cambridge Quartely of Healthcare Ethics, October 2011 20 : pp 584-595.

[50] For an overview of national controversies, see The LSE Identity Project Report: June 2005, pp. 45-97. Retrieved from http://is2.lse.ac.uk/idcard/identityreport.pdf

[51] http://en.wikipedia.org/wiki/Policy_laundering

First, as just described, the most important ***policy decisions*** have been made in the highest of levels and, to great extents, been marked by secrecy. A 2007 House of Lords Report on the SIS II specifically criticised the lack of transparency in Council proceedings[52]. This assessment was made on the background of the observation that it had proved

"difficult for parliaments and civil society to obtain any access to texts under discussion, or to follow the progress of negotiations between the Council and the European Parliament. JUSTICE pointed out the…notorious difficulty for non-governmental organisations ... to obtain up-to-date information about the current state of Commission proposals for legal instruments, such as SIS II, under negotiation in the EU Council". The situation is complicated because when the European Parliament and the Council seek to agree on legislation at the "first reading" of the co-decision process, there is no formal or even informal arrangement governing the conduct of their negotiations".

Second, difficulties such as these were no doubt connected to security issues at stake, but could also be related to sheer ***technical and legal complexity***: The EP LIBE background report describes the SIS II as a *"complex and opaque project – hard to understand, even for experts and absolutely incomprehensible to citizens"*[53]. This even goes for the Commission itself, which, in commenting upon delays of the SIS II stated that *"the complexity of the project itself also had a negative impact on the planning*[54]*".* Such issues of systems complexity clearly relate to the scale of biometric systems now being implemented. If it be the case that systems are bugged by a number of unresolved technical issues, and if these furthermore are not communicated: how can one expect an "enlightened public debate" to take place?

Third, on the side of industry, and in the scientific and engineering community of biometrics, a ***"deficit model" of biometrics' users*** has been, and remains, prevalent. When it comes to large-scale biometric systems issues of public perception and acceptability cannot be ignored: without subjects' cooperation they will not work. However, acceptance of systems already implemented is predicated on the prior acceptance of the over-all biometric imaginary: In order for acceptance and enlightened debate to take place, society must be educated. This was clearly articulated in a joint EC/industry report that tried to assess the experiences with the implementation of large-scale biometric systems in Europe to-date (i.e. 2008):

"There is a need for initiatives leading to widespread public awareness amongst EU citizens as to the purpose and use of biometric technologies in large schemes such as e-passport and public administration applications. If the purpose of the system is clearly explained to the citizen, and also the way the citizen is expected to interact with the system, and if the safeguards are in place with their resulting benefits, all stakeholders involved would be in a better position to understand their role in biometrics deployment. A fair and open debate could then commence with discussions on costs/benefits, purpose of systems, potential impacts, in the long run ensuring system take-up and use"[55]

Industry, engineers and scientists generally remain committed to a "deficit view" (Irwin and Wynne), of publics and citizens as users. The mechanism here is as simple as it is banal: when seen from within the biometrics imaginary, people who do not accept, know or understand the fundamental principles of the technology, are ignorant and to be educated. As can be seen from the above quote, an "open debate" is encouraged, but this is predicated on the prior acceptance of the basic premises, i.e. that biometrics promotes security and user friendliness, while protecting or even enhancing privacy and

[52] House of Lords 2007. 'Schengen Information System II (SIS II). Report with Evidence'. London: House of Lords, European Union Committee.
[53] LIBE 2004
[54] House of Lords 2007
[55] Goldstein et al. 2008. "Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats". European Commission, Joint Research Centre Institute for Prospective Technological Studies, Seville.

freedom of movement. This "forced character" of the premises of a public debate are paralleled by the lack of opportunity to opt out of emerging biometric systems. As remarked by Margit Sutrop, in the governance of large-scale information systems it seems that we have moved from informed consent (biobanks), to presumed consent (electronic health registries), finally to arrive at no consent (biometric systems)[56].

A different though related problem is this: between the level of citizens as users and high-level policy makers there is another (essential) level of actors, namely those intended to implement and operate the systems: engineers and software developers, but also officials such as immigration officers, border guards and law enforcement agencies. A main issue with interoperable systems is that these groups of operators and their related institutions should be made to communicate, exchange information and collaborate. However, in practice serious problems emerge as operators are expected to collaborate across national legislatures, operational cultures and borders. In 2006 the Commission diagnosed the following problem relating to the implementation, testing and operation of systems: *"…wider and more direct consultation with Member States and exchange of best practices would be useful…more consistent introduction and use of certain data…should be made by Member States"* (European Commission 2005). Problems relating to such lacking exchange of information were repeated in a 2009 communication from the Council. At this point in time, the SIS II implementation was in a state of deep crisis, to the extent that an alternative plan was developed for the case that the initial system had to be abandoned. A key issue identified in the *SIS II analysis and repair plan* was the low level of participation among member states in testing the system (European Council 2009). Similar issues were emphasised in the already mentioned 2008 EC/industry report:

"One overall recommendation for EU policy-makers is to create consensus among the Member States and implement a procedure that would facilitate the open dissemination of all information on biometrics systems in the implementation phase. This lack of information concerning EU Member States large-scale projects does not bode well for biometrics deployment in the future as keeping this data secret could suggest that the systems are not secure, may hide poor error rates, be behind schedule or conceal unsatisfactory roll-out results" [57].

Taken together, the last two quotes illustrate part of the problems relating to the strong top-down character of implementing biometrics in the European Union and its member states.

We now turn to a description of some of the alternative imaginaries emerging through the Technolife forum. As we shall see, participants turned out to be fully capable of grasping important ethical and political aspects of the technology. However, the debate suffered from concrete issues to give it a more tangible content. Discussions and policies should reflect actual user-cases and norms of specific context, which are demanding that information processing should be appropriate to that context and obey the governing norms of distribution within it [58]. Also, for the participants and for experts it were much easier to understand and discuss the implications and benefits/risks for individuals and society using the case examples. Contextual understanding is crucial also atin the level of policy making. The effective policy making needs the specific user cases. The point is that user-cases for biometrics are very different and it is impossible to create one policy for all. Thus there is the need for and open discussions at the different levels about the functionality and purpose of biometrics on the basis of user cases[59].

---

[56] Sutrop, M. 2010. Ethical Issues in Governing Biometrics Technologies, retrieved from http://www.springerlink.com/content/978-3-642-12594-2/

[57] Goldman et al. 2008.

[58] H. Nissenbaum, "Privacy as Contextual Integrity," *Washington Law Review* Vol 79, No. 1, February 2004: 119-158.

[59] Snijder, M. (2010). Biometrics and (e-) Identity. How and where to increase the efficacy of the dialogue? Presentation at the RISE workshop "Ethical and Policy Implications of Global Mobility and Security", Brussels, Berlaymont Building on 25 & 26 March 2010. Available: http://www.riseproject.eu/rise-events/workshop-on-ethical-and-policy-implications-of-global-mobility-and-security-brussels.98.html

Indeed, we take this state of affairs to be fairly typical of the democratic and ethical problems and challenges facing responsible developments of biometrics in the European Union, within member states, and beyond.

3. Forum debates: deliberating (in) a policy vacuum?

The forum was facilitated by KerTechno (see …), and invitations were extended to a number of individuals and groups who are considered stakeholders of one kind or another: experts, administrators, relevant occupations, interest groups, and more. We will not, in this report, delve deeper into the invitation and recruitment procedure [60]. In stead, we shall take a look at the forum results from three slightly different, though complementary, perspectives.

In the *first* section we will explore the technology through direct comments to the short film intended to kick-start forum discussions. We especially focus on some of the interpretive and imaginative registers of perception and reaction, and how they respond differently to the frames provided by the film. These registers are anchored in: 1) the ways in which the film **confirms** to participants the necessity of biometric and other information technologies; 2) the ways in which **certainties and uncertainties** about these technologies are **mitigated by participants**, doubts cast and questions asked; 3) the ways in which the film are **seen by participants as "mistaken" depictions of the world** in reference to the use of computing systems, governance and social-ethical costs.

In the *second* section we focus on participants responses to a set of issues selected by us and embedded in the short film. The issues build on a previous scoping exercise, which results make up the main body of the previous sections of this report. Following this exercise, the biometrics and mobility forum was designed to hone in on three focus issues for discussion and debate:

1) **Social justice** - Can biometrics promote freedom of movement, security and justice? Could new mechanisms of exclusion and discrimination be built into these systems?
2) **Surveillance and privacy** - What does "privacy" mean for you? Could biometrics improve privacy and security at the same time?
3) **Trust in technology and in government** - Can governments and operators be entrusted with keeping our personal and biometric information?

In addition to being embedded in the film, the issues were proposed by us in two principal ways: first, they appeared at the entry page to the forum; second, our facilitator would use them to direct and steer deliberations.

In a *third* section we focus on specific imaginaries as articulated by three participants. Whereas a number of participants used the forum to actively explore the issues as well as the character and necessity of the emergence of biometrics, only a few actually reached a stage of a coherent articulation of a comprehensive vision of biometrics and society. Due to the relatively immature stage of technology implementation, as well as the general conditions for an overarching debate (as described in the previous section), this should come as no surprise. Indeed, also those who got to articulate a coherent vision, did so in relative independence of concrete biometric applications. At times, biometrics emerged more as a subspecies of "technology" in general. Still, the general characteristics pointed to in the introduction (a social technology, "seeing like a state"), were clearly grasped by these participants. Hence, the problem would not be so much lacking capacity to comprehend, but rather a lack of concrete issues, applications and information about the technology and its implementation.

[60] See Rommetveit, K., Gunnarsdóttir, K., Jepsen, K. S., Bertilsson, M., Verrax, F. and Strand, R. (in press): "The Technolife Project: An experimental approach to new ethical frameworks for emerging science and technology", The International Journal of Sustainable Development.

3.1. Confirming, questioning and reframing the technology

A narrator in the film makes claims about biometrics, starting at 0.26. *Biometric technologies **are** fast emerging*, *biometrics **can** improve document safety* and *biometrics **can** make travelling faster, easier and safer* (0.26-0.43). Then, in a sequence starting at 1.17, the narrator explains what biometric technologies ***are*** and what they ***will be*** in the near future, *using gait, body odour or even recognising suspicious behaviour and criminal intentions* (1.17-1.43). This last statement overlaps a two phase scene of a "smart" camera dynamically detecting suspicious behaviour in a car park (1.40-1.48). Thereafter, the narrator continues stating what ***can*** *be stored in vast central computers* and concludes with an affirmative remark: *collect information, connect the dots, gain control* (2.01-2.04).

It is noteworthy that the sequence *about* biometrics (0.26-0.43), immediately follows narration which has just stated how difficult it is to keep track of individuals (0.10-0.22). Also, the sequence where the narrator *explains* biometrics and how information can be gathered (1.17-2.04), follows immediately a question of who can be trusted and who is a threat, and the claim that more and more information about individuals is made available to government and business (0.46-1.09). This particular juxtaposition in the voice narration—of uncertainties on the one hand and, on the other hand, statements about what biometrics are, what they do and what that means, i.e., *control* (0.26-2.04)—performs a vision of the near future with some authority. The narrator is located and speaking from within "our" world as the images indicate (see next paragraph), about particular kinds of uncertainties and imminent technical measures to curtail the risks and dangers. This is a persuasive message which is reinforced during the last minute of the film (3.08-3.55). A computer voice quotes Chertoff's vision (former US secretary of state, see page 4), now located and speaking on the outside of "our" world as the images indicate, about security envelopes for free trade and travel for "us" (the trusted) so that "our" resources can be focused on those "outside" who want to harm "us".

In these ways (and others), important premises of EU biometrics policies and technological developments are packed into a film of only 4 minutes of duration. What supports the reading of the film as engaging with the social and technical *imaginary*, is how this vision of the near future is indicated by participants who comment: *"**This is a vision of a** (in my opinion very near) **future** where a lot of information can be connected from very different source to track the actions and movement of people"* or *"**This film emphasizes** my feeling that **we are entering new territory**"*. Arguably, this imaginary is also emotionally charged. The words of the narrator are persuasive and authoritative—biometrics are, can, and will be.

3.1.1. Confirming necessity

In some of the direct responses to the film, we observe claims about the necessity or even the inevitability of biometric technologies. As evidenced in most contributions to the forum, participants state their *beliefs*, *points of view*, *opinions*, what they *feel* and *think* in first person. Also, they state where *we* are at, what is *ours*, what *we* have to do, what governments or authorities *will do*, *must do*, *will not do* or *should not do* and, finally, what *will be*, what *is needed* and what *should change*. The following two fragments illustrate how this happens in reference to confirmations of necessity.

Anne
[…] the video and its topic is **something we all have to** relate to in the future to come, and **it is my point of view** that the use of this kind of technology **is bound to** occur. **It will be** implemented widely […] and **I believe** the intentions are good. […] **I do welcome** this opportunity to easily identify people […] **we must** allow the authorities to identify the people who are here illegaly […] As **the governments implement this** technologies, **it is my belief** that **it will do us** no harm, rather than make the society as a whole more secure and more transparent. **I think** this is a new technology for the future that **the authorities will use** wisely […] it is only the paranoid among us who question this progress.

Brian

[…] extremely strong constraints **need to exist** to prevent one individual from causing massive causualties. In today's liberal democracies, individual rights seem to be maximized, ignoring the danger to the group from such a short-sighted policy. […] **In my opinion**, it is a crime against the citizens of a country that it's government doesn't know exactly who is in the country at any given minute and the personality profiles of everyone (and keeping much closer track of those deemed to be potentially dangerous). […] Biometric data, cameras, and monitoring of communications is but a few of the very necessary **steps the government must take** to assure the continued safety and well being of it's citizens. […] the video prefacing this forum was designed to push the hot buttons of 'privacy advocates,' […] **All it did for me** was demonstrate how far **our society needs to go** just to protect the group from demonstrable threats that exist today. That video just shows that **we have a long long long way** to forming the psychological paradigms (and infrastructure ones too) that **will be necessary** to support the high technology society that is starting to grow **around us**.

What these two contributions have in common is first that neither poses a question. Rather, both state clearly opinions and beliefs that take the narration in the film at face value in the sense that the film shows us "something we all have to relate to […] the use of this kind of technology is bound to occur" (lines 2-3). The film also "demonstrate[s] how far our society needs to go just to protect the group from demonstrable threats". This line of reasoning may seem to put meaning-making to rest. The social semiotics that are perceived and responded to by Anne and Brian draw on very particular assumptions about "us" and "others" who are illustrated in the film as black persons in underdeveloped settings by Western standards. There are particular assumptions about uncertainties relating to any individual (e.g. who they are, what they do), about risk (e.g. who should be let to pass easily), about danger (e.g. those who want to harm us), and about control (e.g. use biometrics, collect information, track individuals). Both Anne and Brian produce comments which are complementary to and align with these particular assumptions.

3.1.2. Raising questions

Contributions that perform doubt sometimes raise actual questions, asking why, who, where, what, are we, is it, doesn't that, and so on—sentences finished with question marks. For example, we observe that mitigations relating to abuse and safety regulations are articulated in open lines of enquiry.

Emilia
It is really good in some sense. It is easier to travel, make document, ...**But, what with** privacy**? Is it possible** to make some kind of turn off/on switch**?** If I want to be identified than I will [be] tuned on. In same other cases I will turn off.

Frank
Very interesting systems, **the question would be** hat **if I would** be more safety about this **or what could happen if** somebody else take my identity and us in a bad way**?**

Apart from the fact that these contributions perform scepticism (*but*, *what if*, *what could*, etc.), the actual formulations of enquiry hone in on specific concerns which are personal but incomplete. They do not offer *an opinion* or *a point of view*, a *belief* or what *is needed*, in relation to these concerns, but they perform sentiments that anchor *personal need* for privacy (Emilia) and a *feeling* that safety may not be achieved for *me* (Frank). The ways in which these sentiments are expressed using question marks, leaves them open to further enquiry.

We observe how openness to further enquiry is similarly evident in responses to the film in which participants also indicate clearly that they are informed and knowledgeable rather than say, gullible. This method of expression persuasively grants authority to the enquiries that follow and ask, for instance, whether or not the technology actually works, if we can trust it or why there is little debate. Consider these two examples:

Heather
But **I do wonder** about our increasing desire for more information and speed, […] I can **only guess** in **the haste to implement this programme no thorough review of EU law was conducted**. My point is, I suppose, this stuff often doesn't work; […] **I question** how we handle and manage, in this case, information and speed.

Ian
Who decides who can be within this security envelope? **What requirements and restrictions** are imposed and to what extent? Moreover, **if one of the thrusts of the European Union is social cohesion**, **doesn't this** idea in general exclude rather than include?

Heather first raises a doubt "I do wonder" (line 2) and Ian first asks two questions, "who decides" and "what requirements and restrictions" (lines 9-10). Both are then followed by observations about the EU. Heather makes explicit that EU countries were in a "haste to implement this programme [biometric documents]" and that a "thorough review of EU law" might be missing, "I can only guess" (lines 2-4). Heather's concern turns on a question about the handling and management of information and speed. Ian, on the other hand, makes explicit that "social cohesion" is presumably (using an *if* clause) "one of the thrusts of the European Union" (lines 10-11), to question decisions about requirements and restrictions for inclusion in a security envelope, "doesn't this idea [this security envelope] in general exclude rather than include?" (lines 11-12).

By first raising doubt or questions, Heather and Ian open lines of argumentation, presupposing that a *general enquiry* is indeed needed. These presuppositions are then supported with observations that lead to further, more *specific enquiries*. Heather wonders about a (general) desire and then asks how its objectives can be handled and managed in relation to what can be observed about EU practices, "this stuff often doesn't work" (line 4). Ian asks (generally) who decides and what the requirements and restrictions are, and then asks in direct reference to an EU objective, whether indeed that objective is met.

By raising questions, participants actively advance the meaning-making which is initiated in the composition of the film. There are particular uncertainties relating to these added assumptions (e.g., is this safe; does it work; who decides), also risks (e.g. identities can be stolen; people can be unfairly excluded), danger (e.g. if problems and potential uses are not debated or the law is not adequately reviewed), and control (e.g. control over inclusion and exclusion; control over private information, control of someone else's identity). In other words, participants produce comments and questions which align concerns and uneasiness with their own assumptions and, thereby, they not only progress the world-making that already is evident in the film but actively draw on their own resources by naming what they *think*, *feel*, *believe* and *know*, i.e., engage creatively in meaning-making which *demands* further development.

3.1.2. Performing critiques

Among the contributions that were discrediting of computing systems and governance, the most succinct questions are perhaps not surprising: "What would it be like if an authoritarian government could have access to this kind of information? […] we could perhaps not exclude that possibility?". This is a common and recurring theme in public and professional debates as well as in media representations of the information society and the practices surrounding the management of information about citizens. Nazi practices are often alluded to, or specifically mentioned, to argue that these continue to be legitimate questions. Contributions which are perhaps not surprising either, are directed at computing systems in reference to dark science fiction about preventative governance to protect citizens: "Are we sure we want a 'Minority Report' future?! Are we sure that the 'Central Computer' is really trustable? Why using biometric to match someone?". This is also a common and recurring theme in public and professional debates as well as in media representations of authorities seeking to prevent crime or terrorist attack.

We also observe profound disillusions with the current socio-economic, technological and political

landscape, directed at the economic leadership of Western democracies. Consider this example:

Jay
Instead of asking how could new technologies erase borders and lower worldwide inequalities and questioning current (outdated and dieing) socio-economic system, **they** [the film] **babble about terrorists, security threats and other symptoms**. […] Full positive utilization of those technologies is impossible until we answer some bigger questions. Like: **How can we** delegate decision making to machines? (resource management for example) **Are we done with** perpetual 'growth' economy and consumerism? **What makes** human life good in most practical sense? **Can we** finally abolish rat race we are constantly pushed in despite industrial automation, technology and abundance? **How can we** minimize and eventually make politics obsolete? **Are we done with** full employment spin and long dead economics? **Are we done with** economy that is unsustainable without continuous wars and militarism?"

Jay takes a sharp turn in meaning-making by depicting a world which is dominated by an "(outdated and dieing) socio-economic system" and riddled with the symptoms thereof, the most obvious being terrorists and security threats. What Jay offers is a significant challenge to certain continuity in common reasoning on the matters of security and the use of biometric systems. Jay achieves this by carefully orienting the reader away from the film toward specifically named phenomena, *machines*, *human life*, *rat race*, *politics* and *economy*, embedded in formulations of a series of questions, in which these phenomena as cast in terms of *decision delegation* (machines), *practical good* (human life), *business-as-ususal in spite of industrial automation, technology and abundance* (rat race), *obsolescence* (politics) and *perpetual unsustainable 'growth', consumerism, full employment spin, warfare and militarism* (economy). Questions are developed here by way of reasoning and enquiry in which particular phenomena are named and cast in terms that substantiate credence to a core claim and furnish it with social-ethical relevance.

3.2. Deliberating the issues

In addition to questions over technological necessity the forum also offers the three focus issues to further guide participants and some of the responses to the focus issues are on a continuum with responses to the films. As the focus issues take shape, participants also shift the aim of their contributions to address additional questions, problems, concerns, and so on.

3.2.1. Social justice

We first see how questions of social justice are anchored in contributions which touch on issues of fairness, state abuse, technical system errors, or the perceived necessity to apply biometric technologies to have control over dangerous individuals. Profiling and social sorting, detection of suspicious behaviours and terrorist threats, are some of the security measures that find expression in participants' statements. For instance, participants who favored biometrics as a necessary tool for ensuring social coherence put the following type of arguments forward:

Jacques
I would like to remind you that **1 in 20 people (estimate) are psychopaths** [...] it does mean that there is a significant number of people in our society that have the emotional and psychological **freedom to commit unspeakable crimes** if they choose to. As an example, the genomic revolution enables individuals to construct highly contagious extremely lethal virus. A severe pandemic would cause our civilization to collapse, killing billions. Don't believe me? Check out the paper "The Darker Bioweapons Future" written by the CIA (unclassified). **Don't underestimate the power of an individual** even in this pre-high technology society to destroy the group. The power of the individual will only grow **as our technology becomes more advanced**.

Kevin
I would think that the **majority would want closer monitoring and control of everyone so as to**

be protected from the minority.

More intrusive security is associated with high-risk individuals who need to be detected and controlled by governments. The power of the dangerous individual is seen to correlate with advancing technologies, and majority rule over minority to monitor everyone is recruited on the assumption that the majority really wants to be subjected to surveillance in order to be protected from a dangerous minority. On the other hand, other participants would underscore the impossibility of control, and so question the course suggested by the above quotes:

Hillary
The hardcore criminals will always find a way to subvert any security system. **Security measures never eradicate all criminals**, at the best minor criminals are stopped while the major criminals continue to function. At the worst **innocent people suffer due to the enhanced security**.

We also observe how the threatening individual is referred to as *criminal*, *psychopath*, a *minority* or simply *those*, and the victims are *innocent people*, *our civilisation*, *the group*, *the majority* or *billions*. Best and worst case scenarios are weighted against each other to casts doubt on the effectiveness of the new security systems.

3.2.2. Surveillance and privacy

Questions of surveillance and privacy are anchored in concerns about respect for individuals, breach of privacy, having control or protection, trust, and the purpose of the technology, i.e., concerns which give privacy meaning and relevance. What counts as privacy appears notoriously difficult for participants to clarify except in reference to either breach or control—that persons have reasonable control over who can access them or information about them, what precisely is accessed and for what purposes.

Noam
I think everyday we release a lot of private information. **The import thing** is **to know what are the consequences** of releasing that information and **being free to decide** if we want to release it or not. First of all I think **people should be informed about what kind of information** they are releasing, **their impacts in terms of privacy and security**, when giving their biometric data. When delivering this information **it should be clear who and when** it would be used. […] For governamental organizations […] **they should be allowed** to use that information if needed. **Probably by using biometrics** the **public security could improve**. But **biometrics will be an issue to privacy** in any case. The **question is, the increase in security compensates the privacy losses?**

This was one of very few cases in which the "balancing metaphor" (see section…) actually occurred. Having control however, appears to many participants to be void of meaning in a world in which most activities are easily intercepted, and any data that can be gathered is, in all likelihood, gathered by some agency, overtly or covertly, processed, disseminated, and so on. We also see that questions of surveillance and privacy are anchored in contributions that doubt if high degree of privacy is desirable. Participants discuss the consequences of issuing personal/private information or being free to decide whether or not to give it away, having some protection, and distinguishing between different purposes for which the information is used (government, workplace, business). They raise questions about legality and confidentiality agreements, and discuss if private companies should be allowed to collect sensitive information, if one should give information away simply if one is requested to do so, or if government agencies should be allowed to exchange the information.

The facilitator attempted more than once to hone in on the question of "what privacy means for you". First, two days in a row under the subject "biometric uses", the facilitator asks five questions: What does "privacy" mean for you? Is it threatened by biometrics? [...] Is it ok for you that you give biometric data to governments any time a police officer request it? Is it ok for you that governments exchange this information? Is it ok that private companies collect this data?

The nearest we come to a direct response to the first question is this:

Quine
For me **it means being able to move freely**, especially in public spaces (online and offline). I believe

public spaces are threatened and in need of being defended. This also goes for ICCTV and similar applications.

Jay

Very complex topic. […] it highly **depends which world we have in mind**. In current world, where **everything has a price tag** and is for sale, I am afraid that aggressive implementation of biometric technologies (not just passports) would just lower the "price" of **already devalued human life.**

Quine defines privacy as freedom of movement, "especially in public spaces (online and offline)" (line 2), followed by concern that "public spaces are threatened and in need of being defended" (line 3). From this we can assume that "not moving freely" would be caused by interception and interference, infringing on the person's privacy. Regina, on the other hand, states that privacy is a "[v]ery complex topic", depending on the "world we have in mind" (line 8). But we have to guess that the references to "price tag" and "already devalued human life", indicate that the value of privacy is also lowered with aggressive implementation of biometric technologies.

3.2.3. Trust in technology and in government

The focus issue on trust in technology and in government overlaps with the other two focus issues, but it is more specifically anchored in concerns about the systematic sharing of information and knowledge which is achieved by organising and streamlining protocols, practices and connectivity for better synergy and data availability to various EU agencies and beyond. Participants discuss if this is the direction in which the use of databases is heading (including the use of biometry), and if data protection directives can actually protect citizens or if are they mainly smokescreens. Participants discuss if we can separate meaningful utilisation of biometrics systems from the centralisation of biometric data, and privacy-enhancing options came up, i.e., if data collection should be minimised or if the purposes for which data-use is permissible should be minimised. The issue of trusting governments draws attention to governing practices in relation to the individual but also to the sorting of individuals into groups. Rather than perceiving strictly of governments as dangerous to individuals, participants point out the measures already in place (including the use of biometry) to sort people with implications for (in)equality, (un)fairness and (dis)crimination. Furthermore, participants discuss the risks when interest groups seek to further their purposes with respect to particular "types" of individuals, ie., the "subsumption of individuals under certain groups […] strong power interests, or distinctions that are made more or less by random".

In a number of entries participants also actually displayed an open distrust of governments. Typical for all three research lines we found the perception that such distrust is grounded, not necessarily in the corrupted or power-abusing character of officers (although this was also expressed), but rather as grounded in a social analysis. In short, prevailing institutions were seen as belonging to a by-gone age, as dysfunctional and in need of replacement. Consider the following two entries:

Jay

"Why is there so little genuine debate on real causes of current crisis, biometrics, genetic engineering, consumption, fundamental economy? I cannot find any other cause but inertia. Inertia of outdated elitist doctrine of treating people like little kids who are unwilling/unable to accept complexity"

Hillary

The main problem is lack of trust. Lack of trust is particularly a problem regarding Governments. **If we could trust Governments and if we could trust people in our communities then we would have little need for privacy**.

PRIVACY IS CRUCIAL AND PRIVACY FROM GOVERNMENTS IS THE MOST NEEDED PRIVACY

3. 3. Three visions

The above two section have focused on aspects of our sociological analysis of the Technolife biometrics forum, corresponding to the projects Work Package 4 (for the full analysis, see TECHNOLIFE deliverable D4.1). What is noteworthy from this analysis is a relative lack of structured issues or themes. Or, in other words: among participants different points of views there is a lack of stabilisation, which again makes it difficult to make decisive statements about the main concepts deployed by Technolife, i.e. *imaginaries*, *socio-technical imaginaries* and *imagined communities*. Now, this may reflect back on the methodology used, as well as the general performance of the Technolife team. There are undoubtedly a number of tasks and processes that could have been handled differently and with greater skill in the course of executing the project. At the same time: The procedure followed is pretty much the same as in the other two research lines. In the BODY line of research, we did manage to "collect" a number of imaginaries, some of which were shared among many participants and can also be found in public debates, on web forums etc. Hence, a plausible explanation is that a public debate over biometrics at a European level is difficult to perform. This is so because of: 1) the technology is only recently emerging at the scale and depth now being seen; 2) as noticed in the introductory sections, and as also noticed by a number of other observers (Lodge, Bigo, Lyon, etc.): deliberations over biometrics take place in a policy vacuum. This much was actually articulated by one of our participants during discussions over privacy. Another participant gave concrete examples from privacy law, whereupon the answer was that:

Jay

"I like this practical approach with examples. Maybe (the facilitator) could bring some more facts, possible plans or exact spots? That way we could avoid wandering around in relatively empty space and discuss concrete problems with the big picture in mind"

There is a lack of information, and there is a lack of *publically articulated issues* that may be used as reservoirs for further meaning making, not to say the possible sparking of broader publics into being [61]. It is a well-known fact that privacy and surveillance related issues do not correspond with the emergence patterns known from other technologies, such as stem cells or GMOs, where relatively broad coalitions have been mobilised in response to techno-cultural developments. Instead, advocacy and activism take place in relatively small and fast-changing (global) networks, frequently promoted by people belonging to cultural elites [62].

Still, and as already mentioned, (at least) three participants, including "Jay", actually did articulate comprehensive visions, or imaginaries, of biometrics and society. Conceptually, we prefer to use the term "visions", since these were, within the forum, single articulations provided by individual participants. Imaginaries, on the other hand, are collective representations [63](Taylor 2004). And, to make reference to Jasanoff and Kim's concept of socio-technical imaginaries, these must refer to some attainable course of action. Such action must be broadly understood, as giving some general directionality to technological projects[64]. The visions we are about to present could be said to correspond to views existing "out there" in some segment or other of globalised cultures. In that

[61] Marres, N. 2005. Issues spark a public into being. A key but often forgotten point of the Lippmann-Dewey debate. In: *Masking Things Public*, Bruno Latour and Peter Weibel (eds.), MIT Press, Cambridge MA.
[62] Bennett, C. 2008. The Privacy Advocates. Resisting the Spread of Surveillance. The MIT Press, Cambridge MA.
[63] C. Taylor, Modern Social Imaginaries, Duke University Press, Durham and London, 2004.
[64] S. Jasanoff, S.-Y. Kim, Containing the Atom: Sociotechnical Imaginaries and Nuclear Power in the United States and South Korea, Minerva, Online 26 June 2009.

respect they refer to socio-technical imaginaries. In terms of empirical data, however, they are single cases and so we stick with the concept of visions. Hence: three comprehensive visions pointing towards wider cultural and global imaginaries. Our three visions *could* qualify as socio-technical imaginaries if shared by a sufficient number of people and if implemented in concrete practices. They are comprehensive insofar as they: 1) identify critical conditions that pose decisive challenges to societies (both Europe-wise and globally); 2) situate biometrics within the wider framework of such challenges, either as a solution or as a hindrance to solution; 3) set out a wider vision of where society and technology is, or should be, heading. We shall keep commentaries brief, and to the greatest possible extent let our participants explain themselves:

3.3.1. Hillary: Governments and capitalism is the problem

"There is nothing good about biometrics because biometrics are open to misuse. Biometrics is simply a tool of oppression, but the leaders of capitalism say biometrics is for our safety and it will speed up everyday processes. We are told these measures will help prevent terrorism but we often see laws designed to stop terrorists being applied to people how are engaging in lawful protest. Anti-terror laws are a way for corrupt governments to silence freedom of expression. Biometrics is the beginning of 1984, it will lead to thought-crime and other authoritarian methods of oppression…"

Much commentary is not needed here: governments are corrupted by capitalism, and they lie to their citizens about the purposes of the technology. Terrorism is the main justification for the oppression of citizens performing their rights. The reference to 1984 is of course well known, and frequently referred to by privacy activists, libertarians and anarchists [65]. On this view, biometrics is, almost per definition, inscribed with such negative intentions and values (seemingly irrespective of cultural context, modes of employment, etc.). Some more detail is added, insofar as the critique of capitalism is connected to a certain views of ownership, and insofar as ownership is connected to control and power:

"Capitalism seeks to create masses of stupid people (blissfully unaware people) who will happily accept lower wages. CEOs, directors, Leaders etc receive gargantuan wages while the Masses receive very small wages therefore a lack of intelligence is essential so that the Masses do not question this disparity of wealth"

This, then, would go some way on casting a light on why, during the introductory phases of biometrics in Europe, so much information and so many crucial processes have been withdrawn from public scrutiny. Finally, Hillary envisions a set of possible solutions to our dire predicament. One continues the reference to political economy, insofar as a new phase of developments, mainly driven by ICTs and networking technologies, will/ought to be ushered in:

"In a world of Post-Scarcity everything will be free, everyone will be supremely powerful, and everyone will be supremely intelligent. Politics, politicians, and corruption will be obsolete in a Post-Scarcity world…there will be no wars because there will be no scarcity of resources to fight over"

This is utopian, for sure, but not more so than that serious authors have spent considerable time pondering the concept: in sociology, Anthony Giddens has made extensive analyses of post-scarcity[66]; it is a recurring theme in science fiction[67] and the internet abounds with speculations about such a

[65] See for instance Statewatch News Online (2004) 'The road to "1984" Part 2. EU: Everyone will have to have their fingerprints taken to get a passport ', (Statewatch News Online).

[66] A. Giddens (1996) 'Affluence, Poverty and the Idea of a Post-Scarcity Society', Development and Change, 27:365-377

[67] See for instance Ian Banks *Culture* novels.

possible state. Currently seen inequalities are tightly bound up with the access to crucial resources, information, and decision-making. Awaiting Post Scarcity, however, Hillary also imagines another line of defence against state and corporate oppression, namely un-conditional privacy protection:

The main problem is lack of trust. Lack of trust is particularly a problem regarding Governments. **If we could trust Governments and if we could trust people in our communities then we would have little need for privacy**.

PRIVACY IS CRUCIAL AND PRIVACY FROM GOVERNMENTS IS THE MOST NEEDED PRIVACY

3.3.2. Jacques: in high-tech societies the collective must be protected against dangerous individuals

We have already described some of the points of view put forward by Jacques. Apart from sharing in a generally favourable view of technology, his position is almost directly opposed to that of Hillary. The government is not the problem, but the solution. The individual, on the other hand, represents a danger to the collective. This has always been so, but it is greatly exacerbated in the high-tech societies now forming around us:

"The current situation is not conducive to a sustainable high technology society. In a high technology society, the individual will have the power to destroy the group using advanced technology. Thus, extremely strong constraints need to exist to prevent one individual from causing massive casualties. In today's liberal democracies, individual rights seem to be maximized, ignoring the danger to the group from such a short-sighted policy"

Jacques does not elaborate on the kind of politics or economy he sees forming. It is a kind of collectivist society, with great powers invested and entrusted in the state:

In my opinion, it is a crime against the citizens of a country that it's government doesn't know exactly who is in the country at any given minute and the personality profiles of everyone (and keeping much closer track of those deemed to be potentially dangerous). Some seem to feel that the government is the enemy - so be it. They can live in a dog-eat-dog wild west country where the strong and unethical can victimize the weak and moral at will, without any significant restraint. In my opinion, the government is suppose to protect the weak against the strong, the powerless from the powerful, and the poor from being taken advantage of by the rich. Biometric data, cameras, and monitoring of communications is but a few of the very necessary steps the government must take to assure the continued safety and well being of it's citizens. I would like to remind you that 1 in 20 people (estimate) are psychopaths"

Whatever one makes of statements such as these: Jacques does point to inherent tendencies of large-scale in formation systems, including biometrics: they seem to promote, and are promoted by, collectivist ideologies, justified by reference to "the common good", "solidarity" and "security":

In today's liberal democracies, individual rights seem to be maximized, ignoring the danger to the group from such a short-sighted policy… PM Thatcher was wrong: we are a society, not just a bunch of individuals

3.3.3. Jay: if we do not change our societal structures and ways of living, the potential of biometrics will be lost

The opinions put forward by Jacques could be seen as radical and incomprehensible to many. However, and as also argued in the preceding sociological analysis: they could also bee seen as linear

accelerations of the present state of affairs. This was the opinion of Jay, who introduced a quite different vision and frame of reference. In direct response to Jacques, he claimed that

"Although you admit that future sustainable high technology society will bear little resemblance with what we have today you are still mixing it with current (and thus changeable) premises. Today's beggar, when given genuine opportunity to live a life of dignity is tomorrow's Wikipedia contributor or open source programmer. Children raised humanely without advertizing brainwashing will become contributors not status starved Wall street parasites and speculants or desperate and infantile army recruits"

On an artificial level, Jay is sharing the system critique of Hillary. However, whereas opposing the collectivist views of Jacques, he also opposed the radical individualism of western societies, including the (almost) exclusive reliance on privacy as a means for regulating technology:

"I would also like to hear exact and precise explanation of what privacy is, in this superficial bearocratic context. I have a feeling that we frequently have random and ambiguous flows of Anglo-American wild-west induced paranoia concerning this question"

Whereas recognising the strong influence of the general economic and institutional environment on technology, decisive factors reside in the ways in which our out-dated societies may catch up with the level of technological advancement in the present (and future). As things are at the moment, both technology and general productivity feed into wasteful and exclusivist systems marked by secrecy and only benefitting a few. However, Jay also puts forward a strong vision in which he sees a prominent role for biometrics:

"Sustainability (which we all hopefully agree about) means that available resources are limited and must be allocated with great care and longterm plans. Biometric tech, as any other tech, has its potential cons but is the only way to make sure that everyone really got their piece of the pie in a high tech society. And its not just about distribution but also of making sure that resources are not wasted in absurd ways. Don't you agree? (I am supposing that we will get out of industrial/state model the same way we got out of explicit slavery/feudalism.)"

Also Jay can be seen to project future states that may seem utopian. However, rather than asking "what he really means", or rather than relying on the realism of some future scenario, it is much more interesting to relate his statements to the present. Indeed, he manages to put the finger on a schism that runs through today's global differences in biometrics deployment, including the ways in which the technology is being perceived by citizens:

"I am not saying that biometric tech is corrupted in western countries. But it is much more prone to fundamental corruption than in underdeveloped ones. Its much harder to harm (with biometrics) those who live in tents and are poor but pretty independent than those whose lives are infinitely entangled with housing/banks/politics/advertising/consumption/job/markets/media.. Role of biometrics in developed world should be exactly the same as in third world just on a different scale"

Anybody doubting the relevance of this insight should cast a glance on the ways in which biometrics is implemented and imagined in India (see for instance the article and interactive features at http://www.nytimes.com/2011/09/02/world/asia/02india.html?pagewanted=all). The following excerpt is representative of the kinds of stories being told:

A worker guided Mr. Gangar's rough fingers to the glowing green surface of a scanner to record his fingerprints. He peered into an iris scanner shaped like binoculars that captured the unique patterns of his eyes. With that, Mr. Gangar would be assigned a 12-digit number, the first official proof that he exists. He can use the number, along with a thumbprint, to identify himself anywhere in the country. It will allow him to gain access to welfare benefits, open a bank account or get a cellphone far from his home village, something that is still impossible for many people in India.

In short, and as we have seen: biometrics in the West has (largely) entered the popular imagination through the lenses of securitisation, strongly enhanced by 9/11. Because westerners are already entangled in a number of goods, services, rights and infrastructures, biometrics is frequently imagined as *taking something away* from citizens. The secrecy of the process of introduction does not help this perception, but rather fuels it. Let us compare the Indian story with an example from Europe: the right to vote. Spain has long since introduced both biometric passports and national ID cards (Lyon and Bennet 2009). However, in the upcoming 2011 elections, more than a million Spaniards living outside their country may effectively loose their right to vote because they *cannot get their papers* from their local election offices in time (http://www.elmundo.es/elmundo/2011/11/16/espana/1321432363.html). Why invest in expensive technology if it is not put to its best use, i.e. to provide citizens with their most fundamental rights? We know that, in several European countries such as Holland, the right to vote has become connected to enrolment in national biometric databases. Why, under these circumstances, should people feel that biometrics *gives them something*, rather than being the agent that *takes something away* from them? This example, suggested to us by Jay, illustrates the strong dependence of biometrics on the wider social setting and imaginary within which it emerges. It also suggests some of the great challenges faced by policy makers, publics, citizens and technology developers in providing more sustainable patterns of co-producing biometrics and societies. The implementation of biometrics in the West does not, as in India, radiate willingness to enable, to collaborate or to provide (issues of high importance in these times of crisis). Rather, the technology and its trajectory seem to be inscribed with decisive levels of distrust towards citizens. Although this is not the whole, or the only story, it may take hard work to cleanse biometrics in the west of this impression.

4. Recommendations for policy.

1. **The best way of promoting sustainable innovation in biometric technologies is a precautionary attitude oriented towards openness, transparency and the safeguarding of civil rights. Biometrics is deeply embedded in social and cultural relations. This makes it highly susceptible to swings in perceptions and the wider imagination. Single events can have great influence, and trigger or change public opinion formations in rapid and unpredictable ways.**

A great number of analysts have already noted, frequently in highly critical terms, the un-democratic nature of the process introducing biometrics in the European Union. This also emerges from our analysis: the biometrics imaginary has been promoted in the highest of political levels by politicians looking for solutions to emergency-like problems, but also fuelled by highly optimistic promises of engineers, scientists and industry. Adding to this, our forum quotes have demonstrated that **broad societal, economic and political contexts *matter to people* in trying to make sense of biometrics**. Uncertain and unchartered landscapes are explored on a number of levels, ranging from privacy, the character and "necessity" of the technology, and the overarching social, economical and technological tendencies and structures within which it emerges.

Most Europeans, as well as visitors to Europe, already have biometrics in their travel documents and passports. However, the wider information structures to which these are/will be connected are still being constructed. In systems such as the VIS, and the coming SIS II, the shift towards biometric searches (as opposed to alphanumerical searches) still has not materialised. In relation to these (expected, promised) developments, public perception and acceptance/non-acceptance remains poorly understood. Both our analysis of public debate(s) and our forum debates (including attempts to recruit participants) speak about a policy vacuum, in which concrete applications and issues still have not materialised.

Great uncertainties attach to the general cultural climate within which biometrics has been ushered in. The killing of Bin Laden and the Arab Spring have changed the security imaginary: the Arab "other" as a terrorist, so prominent in the early days after 9/11, has been replaced by demonstrators in Tahir Square. It *may* seem that the face of terror (Bin Laden) has been eradicated, and replaced by "normal people" fighting for civil rights and a decent living. At the same time, a number of recent cases, for instance in Germany and Norway, have demonstrated how security agencies have overtly focused on Arabs as the threat, whereas by and large ignoring domestic right-wing extremists. If it is the case, as our analysis shows, that the broader context matters to how people conceive of biometric technologies, great care and caution should be taken in the further implementation of systems. Which are the ethnic and cultural presuppositions being built into emerging systems, and how do these correspond with fast changing cultural perceptions and imaginations?

Taken together, this does not bode well for engagements with further developments, making them highly unpredictable and susceptible to a wide range of factors: what if citizens, and those expected to implement and operate biometric technologies, do not behave as prescribed by the biometrics imaginary? A number of recent experiences (i.e. Climategate, Wikileaks, etc.) have showed that, especially when it comes to ICTs, people who are excluded find ways to make an influence, for instance by hacking biometric passports (which already happened on a number of occasions). In the future we are likely to see more hacker attacks on surveillance systems. A way of avoiding this would be to promote much greater degrees of openness and transparency in the implementation and operation of systems. The transparency of the process and inclusion of the public is very important for securing the trust of the public. The lack of knowledge and understanding of possible benefits and drawbacks of new technologies makes it difficult to build and maintain authentic public trust, which is of crucial importance for good ethical governance of databases.

2. **There is a great need to foster greater reflection and awareness of social and ethical issues among scientists and engineers, who frequently seem to operate in insulated and closed-off arenas of opinion making, technology development and innovation.** The forum deliberations were characterised by participants testing the ground, of uncertainties and lack of knowledge. However, this is also the case for parliamentarians, privacy advocates, and even engineers and operators working to implement biometric systems in the EU and its member states. Publics and "lay persons" are perfectly capable of grasping important implications of biometrics. It should come as no surprise that lay or public concerns are not necessarily those harboured by expert communities. The communities in question need to be educated in order to understand and implement this state of affairs.

3. **The "balance metaphor" is, in most cases, ill suited as a vehicle for governance and debate.** There is an urgent need to move beyond the state of the art of policy making, to promote concepts and procedures capable of grasping the complex societal and technological character of emerging biometric systems. Governance remains stuck in an out dated and rigid language, taken from international relations, theories of the state and (to some extent) Anglo-Saxon analytical philosophy. Importantly, most developments concern *groups* just as much as they do single individuals. The notion that the security of states, or the whole of the EU, can be grasped as a whole is illusive, especially as the relevant issues revolve around technological matters that are highly uncertain, complex and stretch into a number of cultural and operational contexts. Furthermore, biometric systems do not conceive of users *qua* individuals, but rather as individuals *qua* members of this or that group or collective (bona fide traveller, threat to public order, Chinese, Moroccan, American, etc). This collective dimension is altogether lost in the strong focus on individuals' rights and privacy, and so point towards the need for developing new concepts and methods for conceiving of the interactions of social groups and biometric systems.

4. It is not only about balancing security with privacy. We need to work with a wider picture of values.
The public forum discussion showed that in implementation of biometrics technologies balancing security with privacy is not the only issue as there are also several other values at stake as it came out from the platform discussion. Dependent of the concrete technology, its function and implementation context, biometrics implementation may raise also issues of justice (threat to discrimination or stigmatization), equality, respect of individual moral autonomy, the loss of public trust and other values. The wider implications to the society (as lack of general trust) and changes to the way of living have so far remained practically unnoticed.

5.Discussions about technology and effective policy process should be based on concrete user-cases and technology samples.

In the pluralistic world it is impossible to give any absolute normative requirements about respecting privacy, justice, fairness, democracy and other values protection for all different technologies or even for technologies we call with common name „biometric technologies". The conditionality and contextuality of the implementation of and norms have become evident and therefore specific contexts (that are determining such things like roles, expectations and behavior of people and limits) are important also for working out the best governance model also for the implementation of technologies and leading of information processes. Therefore it is quite difficult to discuss or enable the effective policy making process relying only on the abstract imaginaries of the kind of technology, like ICT or biometrics technology. The imaginaries need to get the input from concrete user-cases and technology samples. The context where the technology is implemented, norms of specific context and the aim of implementation are the solid basis for defining the rules of governing the technology.

As mentioned, the public is perfectly capable of grasping important implications of biometrics, the problem is rather a lack of concrete technological examples, applications and information about the technology and its implementation. Using case examples or information about concrete technology that has or will be implemented, it is much easier to discuss and understand the implications and benefits/risks for individuals or community. Case examples would make it possible to the public to identify and define under what conditions and in which context they would be ready to accept the technology.

6. Assessment of existing ethical frameworks and revisiting the private vs public distinction.

The insights, perceptions and imaginaries of the public serve as valuable input to implementation and evaluation processes of technologies as well as to policies governing technologies guaranteeing the social acceptance. But it is also necessary to provide a conceptual analysis of the values and issues at stake and assess the existing ethical frameworks for their potential to meet the challenges of the new technologies.

One important question is, whether we should and could move away from the opposition from the individual rights based ethical frameworks and the public interest based ethical framework. At the moment the public interest is often set in opposition with the participants' right to privacy and autonomy and in the end it becomes an either-or issue. Instead we should attempt to balance the individual rights and the common good. We need a new ethical framework for handling the provision of public goods such as security and health. However, it is still not very clear how this should happen and so far the move of the focus towards community leads to abandoning of the respect for individual autonomy and overemphasizing the common good. Our analysis has shown that we should be more aware of the potential risks that accompany the employment of this new ethical framework where the concept of public interest/common good plays the major role.

On the other hand we need to move away from an overly simple dichotomy of public versus private. The two categories are not necessarily always in opposition (one does not always have to give up one to gain the other) and there can be a range of political issues involved in definitions of privacies and publics (for example, who gets to speak on behalf of whom, with what consequences). In place of oppositions between, and singular definitions of, public and private we need to research the multiplicity of terms in action and search for proper categories and definitions.