Transdisciplinary approach to the
Emerging **CH**allenges of **NO**vel technologies:
Lifeworld and **I**maginaries in **F**oresight and **E**thics
(TECHNOLIFE)

A project funded by the European Union
under the 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 N° 230381

TECHNOLIFE deliverable D4.1

Social imaginaries and ethical issues in deliberative process on Biometrics

Authors: K. Gunnarsdóttir, A. MacKenzie, B. Wynne - Cesagen, Lancaster University

Contributing partners: Cesagen, Lancaster University, Bergen University, REEDS Lab. (Ex IACA-C3ED), Université de Versailles Saint-Quentin-en-Yvelines.

Introduction

This deliverable reports on the analysis of a virtual forum discussing biometric technologies in relation to mobility. The forum was facilitated by KerTechno (see D3.1)[1], and invitations were extended to a number of individuals and groups who are considered stakeholders of one or another kind: experts, administrators, relevant occupations, interest groups, and more (see D2.0)[2]. Discussions were kick-started with a short provocative film, drawing on the Technolife scoping paper on "Biometrics and the European Border" which underscores a drift in priorities set by the European Council over the past decade (D1.1)[3]. Commitment to freedom, based on human rights, democratic institutions and the rule of law, has been challenged by new strategies to strengthen the area of freedom, security and justice in the European Union with strong emphasis on the development of the shared visa system and other border controls for the Schengen region (European Parliament,1999; Council of the European Union, 2004; European Commission, 2004; Council of the European Union, 2009). As D1.1 points out, this security-led approach depends on the metaphor of striking the right balance between security, freedom and justice, but it struggles to formulate agendas on how privacy and freedoms can be protected in concrete settings. Particular complications arise here against the involvement of judicial and law enforcement authorities in aggregating and disseminating ever more personal information on both citizens and non-citizens. As the scoping paper suggests, striking the right balance "stretches deep into concrete processes and negotiations shaping institutions, legal frameworks and technologies" (cf. D1.1 in Rommetveit et al, 2011).

It is subject to doubt if the securitisation discourse has actually captured the many and complex interactions between citizens, states and intergovernmental alliance. Security has been the trope for promoting or opposing problems of immigration and border control, but very little has been done to engage wider publics, including a range of occupations who could be seen as legitimate stakeholders in both debate and decision-making. Perhaps the biggest challenge for decision-makers is the limit of prediction in forecasting, i.e., ensuring that we actually have a "roadmap" to a safer and more secure Europe. But if we were to cultivate wider participation and more humility in assessment and decision-making, the assumptions on which "security" already rests will have to give way to questions of purpose and direction (see Jasanoff, 2003 on a similar issue). It is also imperative to understand what means are necessary to intercept and influence the use of biometric systems in early stages of development and deployment. As Wynne has pointed out (e.g., Wynne, 1992; Wynne, 1988), the framing of what the problems/issues are, and what should be debated by publics, is typically confined to the imaginations of scientific, technological, policy and institutional expertise. In other words, visions of statehood, control, trust, privacy, belonging, and more, could be further examined in public debates and KerTechno was positioned as an instrument to attempt such an exploration. 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?

Our methodological approach to the forum, the aims of our analysis and a summary of the many disparate findings, are elaborated in the D4.0 introductory report.[4]

1 http://neicts.lancs.ac.uk/pdf/Technolife-D3-1-DocumentationOfKerDST.pdf
2 http://neicts.lancs.ac.uk/pdf/Technolife-D2-TheoreticalFramework.pdf
3 http://neicts.lancs.ac.uk/pdf/Technolife-D1-1-Scoping-Bio.pdf
4 http://neicts.lancs.ac.uk/pdf/Technolife-D4-Introduction.pdf

1. Identifying actors' assumptions

In this section we will first describe the short film intended to kick-start forum discussions. We will address its composition and use as a method. We ask to what extent, if any, the contributions can be said to be guided or influenced by the world-making this film accomplishes as an imaginary and, apart from that, we explore the meaning-making and world-making evident in the material participants were contributing in response or reference to the film.

A summary description hardly begins to unravel what an adequate transcription and analysis can uncover. Among the many fine nuances in the composition of the film, we draw particular attention to the representation of uncertainties juxtaposed with particular technical measures of control. Then we explore some of the interpretive and imaginative registers of perception and reaction. 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 confirms to participants "mistaken" depictions of the world in reference to the use of computing systems, governance and social-ethical costs.

Narration in voice, image and sound

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), 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".

What immediately supports this reading of the film as an *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. Travellers are hard to keep track of. Who can be trusted? Rhetoric and persuasion is also evident in the use of images and sound. For example, the narration (0.10-2.04) runs on top of fast forwarded images of moving crowds (a market place and passage points through transport hubs), stills of surveillance cameras, an aeroplane coming in for landing, a barbed wire fence, a close-up of a passport, the handling of "low-tech" fingerprint paper charts, the electronic scanning of biometrics in progress with animated bright-coloured flashing process indicators, a patrol officer talking on his radio, and more. This imagery is complemented with a fast high-pitched rhythm (4 beats per second) in the foreground, later introducing floating mid-range cords accentuated with bass tones while the beat fades into middle ground before it overtakes the foreground again, and so on. Altogether, images, sound and narration drum up excitement or alarm which is bound to raise concerns or trigger uneasiness, even fear. Particular shifts in the sequence accentuate this. For example, the beat is starkly in the foreground in the opening sequence with occasional bass tone accentuation during the narrator's statement about the uncertainties in keeping track of people. Then it fades swiftly into the middle ground to give the narrator "more room" to make concise statements about what biometrics are about, what they are and do, while mid-range floating cords are introduced along with bass accentuation which builds up tonality and velocity, i.e., a momentum. Images of electronic scanning in progress whiz by at great speed—blinking progress indicators are accompanied with high-pitched beeps and trickles that also indicate stages in this swift "high-tech" process. Entering the last sequence however (3.08-3.55), the sound drops quickly to almost dead silence. The camera travels slowly on a desert road towards a "low-tech" border crossing, driving slowly past an American flag, a shack, a guard, stop signs, and onward. We see images of a high barbed wire fence, surveillance cameras, and people behind fences, the final shot a close-up view of a black person's face leaning on a fence looking through. The colours are sepia-tones for the most part and this limitation in the range of colour, the silence, these "other" bodies, and a computer voice give the scene an eerie feel to it. The viewer has plenty of time (and room in the absence of sound) to absorb the images and the computer quoting Chertoff. An uncanny sort of place is performed here which, like drumming up excitement, can also alarm the viewer to be concerned or somewhat uneasy.

We will come back to an interim section spanning a quarter of the film (2.06-3:07), which plays out in some detail (although fictionally) biometric technologies and dynamic tracking of one individual. The next question to ask in relation to these elements described here (uncertainties juxtaposed with statements about particular technical measures) regards direct responses from participants, and if (and how) concerns or uneasiness can be detected. We have distinguished "direct responses" as the contributions that either name the film or elements in it directly, or we already know are comments made immediately after seeing the film at the ICT2010 conference in Brussels.

Confirming necessity

In some of the direct responses to the film, we observe claims about the necessity or even the inevitability of biometric technologies. But what exactly is necessary and what are the assumptions manifested in claims that are anchored in a particular opinion, belief, statement, sentiment or attitude? 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.

Fragment: ***D4.1.1***

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 oppertunity 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 psychlogical 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". For example, Anne sees a cause for alarm that there are uncertainties about "people who are here illegal[l]y" (line 6). "[W]e must allow the authorities to identify" them (lines 5-6). Brian expresses the concern that "extremely strong constraints need to exist to prevent one individual from causing massive casualties" (lines 14-15). Brian's opinion is that "it is a crime against the citizens" if the "government doesn't know exactly who is in the country", and does not know their "personality profiles", in particular, "of those deemed to be potentially dangerous" (lines 17-20). In other words, both Anne and Brian have seen a confirmation that biometric and other information technologies are necessary, must be implemented, in fact, are bound to occur, and for reasons both of them explicate using affirmatives such as *my point of view*, *my opinion*, *I believe*, and extreme formulations such as *we must*, *we all have to*, *bound to*, *necessary*, and so on. There are potentially dangerous individuals who can harm the group. There are illegal aliens. This is a demonstrable threat and as Anne also states in her final remark, "it is only the paranoid among us who question this progress" (lines 9-10).

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.

Meaning-making is not fixed or predictable, however. For example, we do observe confirmations of the good of biometrics, but articulated in ways that mitigate both certainty and uncertainty. This is anchored in the use of *I think*..., *but*... and *this has*..., *but*...

Fragment: ***D4.1.2***

```
 1  Celia
 2  I think that this would be much better to have it [biometric technologies] since
 3  the world population is getting large and is moving around the globe, but need a
 4  lot of safety regulations.
 5
 6
 7  Dan
 8  Of course this [access to biometric information] has high scope of abuse, but I
 9  feel this technology has a more positive side than negative. To mention one of
10  them, as the video presented, fast processing of travel related issues :)
```

In these comments, we see how mitigation is used in two different ways. First Celia remarks, "I think", using srong formulation that having biometric technologies is "much better" (line 2), and stating a reason why. Then she mitigates, "but [biometric technologies themselves] need a lot of safety regulations" (lines 3-4). Dan however, begins by stating a concern about the "high scope of abuse", then mitigates, "but, I feel this technology has a more positive side than negative" (lines 8-9), followed by an example of why that is the case.

While both of these contributions use strong formulations, *lot of*...(line 4); *high scope*... (line 8), the order in which these formulations sit with *feeling* or *thinking* about the use of biometric technologies and access to biometric information differs. The former invites more questioning while the latter counteracts it. What we see in both cases however, is a shift in reasoning which begins to take into account *potential* lines of enquiry.

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.

Fragment: ***D4.1.3***

```
 1  Emilia
 2  It is really good in some sense. It is easier to travel, make document, ...But,
 3  what with privacy? Is it possible to make some kind of turn off/on switch? If I
 4  want to be identified than I will [be] tuned on. In same other cases I will turn
 5  off.
 6
 7
 8  Frank
 9  Very interesting systems, the question would be hat if I would be more safety
10  about this or what could happen if somebody else take my identity and us in a bad
11  way?
```

Emilia first states what is good. "It is easier to travel, make document[s]" (line 2), then raises two direct questions, "what with privacy? Is it possible" for the person to be *off* as well as *on* (lines 3-5)? Frank also states first an interest in biometric systems and then asks, albeit indirectly, by stating what "the question would be […] if I[there] would be more safe[ty] or what could happen if…", where the latter of these two *if* clauses introduces the possibility of identity theft and abuse (lines 9-10).

What Emilia and Frank have in common is that *interesting* and, *in some sense, good* systems are made subject to questioning, first a general question and then a specific one. Emilia asks about privacy and then a specific question about user control. Depending on circumstance "I will [be] tuned on" or "I will turn off" (lines 4-5). "Is it possible" to have some control over *my* privacy? Frank also states first what a general question would be, i.e., if there would be more safety, and then asks specifically, "what could happen if" *my* identity is stolen and abused?

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 this example:

Fragment: ***D4.1.4***

```
 1  Greg
 2  Governments and business are moving into cyberspace and increasingly regulating
 3  it. Many of the challenges ahead, I belive, is not how to provide more networks
 4  […] but to figure out how to use networks and computers for different (social,
 5  environmental) purposes […]. Biometrics is one such use of networked
 6  intelligence. Used for regulation of mobility it is mainly connected to the
 7  purposes of states, but also of businesses, to maintain secure environments for
 8  trading (cf. the 'security envelope' in the film). Why is there so little debate
 9  about the possible uses and problems of biometrics? From where comes the media
10  silence?
```

It may not be immediately obvious that "the challenges ahead […] to figure out" (lines 3 and 4) is the key to raising the first question, "[w]hy is there so little debate about the possible uses and problems" (lines 8-9). Greg is labouring on more than one front, first by opening a line of argumentation which states that "[g]overnments and business are moving into cyberspace and increasingly regulating it" (lines 2-3), then by demonstrating his awareness that the use of networked intelligence to regulate mobility has to do with the "purposes of states" and "businesses to maintain secure environments" (lines 6-7). In doing this, Greg persuasively orients the reader to state-of-the-art in governance and business i.e., "moving into cyberspace", as well as to issues of regulation which are <u>not</u> limited to cyberspace but have to do with *purposes*. A purpose of states and businesses is to regulate mobility and keep environments secure. This last claim is promptly legitimised by citing the film (lines 7-8). But the first question, which clearly presents a shift in reasoning, draws on a stated belief in reference to

purposes which are named as social, environmental (lines 4-5). Computer and network uses, more specifically here biometric systems, still need figuring out. There are problems as well as undecided uses, as the question clearly articulates. "Why is there so little debate about the possible uses and problems of biometrics?" (lines 8-9), and, furthermore, why the media silence?

Greg labours to articulate his awareness and understanding to raise these questions. He promptly *tells* the reader what governments and businesses are doing, what biometric systems are and what the regulation of mobility connects to. And, in performing a voice of some authority, his belief which draws on what he knows gives credence to the concluding but open questions. We observe a number of variations to this method of reasoning, i.e., to indicate clearly some awareness or knowledge to give credence to a doubt or a question. Consider these two examples:

Fragment: ***D4.1.5***

```
 1  Heather
 2  But I do wonder about our increasing desire for more information and speed, […] I
 3  can only guess in the haste to implement this programme no thorough review of EU
 4  law was conducted. My point is, I suppose, this stuff often doesn't work; […] I
 5  question how we handle and manage, in this case, information and speed.
 6
 7
 8  Ian
 9  Who decides who can be within this security envelope? What requirements and
10  restrictions are imposed and to what extent? Moreover, if one of the thrusts of
11  the European Union is social cohesion, doesn't this idea in general exclude
12  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.

What we establish is that, by raising questions, participants actively advance the meaning-making which is initiated in the composition of the film. For example, Emilia draws on the additional assumption that personal control over privacy is preferable. Frank contributes the assumption that instituting new technologies is <u>not</u> necessarily safe and can be abused. Greg assumes that the main challenges are still to figure out how to use the new technologies for novel purposes. Heather assumes that the EU may not adequately address the law and "this stuff" may not work. Finally, Ian suggests that the EU does not adequately address one of its own key

objectives. 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, the 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.

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. It concerns questions of predictability using invasive technologies to collect information, and the extent to which networked sensory and information systems actually contribute to preventative governance of security and the social order. But, raising these questions in reference to the film, points to an outlook on the future which is potentially dystopian. We observe profound disillusions with the current socio-economic, technological and political landscape, directed at the economic leadership of Western democracies. Consider this example:

Fragment: ***D4.1.6***

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

What is made quite clear in this contribution, is that `"terrorists, security threats and other symptoms"` (line 4), are indeed the symptoms of unresolved issues: how we can `"delegate decision to machines"` (line 6), when there is `"perpetual 'growth' economy and consumerism"` (lines 7-8), `"[w]hat makes human life good in most practical sense"` (line 8), when there is `"rat race we are constantly pushed in"` (line 9), and we put up with obsolete politics and an

unsustainable economy which calls for "continuous wars and militarism" (lines 10-12). Indeed, we should be "asking how could new technologies erase borders and lower worldwide inequalities and questioning current (outdated and dieing) socio-economic system" (lines 2-3).

This line of reasoning introduces assumptions about technology use, economy, politics, rat race, and more, all of which need resolution or the "full positive utilization of those technologies is impossible" (line 5). The film *babbles*. It does not ask the "right" questions. In other words, 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. The film should question an outdated socio-economic system.

We observe variations on this method in many contributions to this forum, but in relation to the film in particular, it also appears in an exchange between two participants on the issue of whether biometrics is a line of defence against safety being in jeopardy. But at this stage it is relevant to address the interim sequence in the film (2.06-2.07).

What the interim sequence adds to the film is a demonstration in considerable detail, albeit fictional, of "smart" detection of suspicious behaviour and the tracking and detection of *who* an individual is: gender, approximate age, recent travels within Europe, recent transactions of card payments and at cash points, criminal record and citizenship (see appendix). The way this is done is by superimposing animated overlay on top of images of the person, first targeted in a crowd, then a close-up of the face, shots of city and country maps, surveillance street view, and more. The animated overlay consists of fingerprint scanning in progress (obtained from remote), blinking progress indicators in large centre-screen type (red and green), red dots on city and country maps indicating tracked locations, as well as tracking indicators in small green type running down the left of the screen from the top left corner. This very busy imagery is accompanied by a cacophony of high-pitched sounds, beeping and trickling, a computer voice communicating process and progress, accentuating voluminous beats shifting the scene, and so on, until the sound fades quickly during a final brief shot of the targeted person, standing in a street, holding up an open passport, superimposed with final system results centre-screen in green type, EU CITIZEN, TRUSTED TRAVELLER.

Arguably, not only does this detection and tracking sequence fuel the imagination of what networked information technologies (including biometrics) could potentially or actually achieve. The sequence gives considerable weight to the depiction in the film of insiders and outsiders, and the idea of security envelopes to regulate mobility. This is picked up and challenged in our last example:

Fragment: ***D4.1.7***

```
 1  Kathryn  (20/09/2010)
 2  I asked myself the question during the video if advanced biometrics has come
 3  about because of increase in 'evilness' of people, or is it because of the
 4  increase in technology that we are able to see the 'evilness' that has always
 5  been at the heart of humankind?
 6
 7
 8  Response from Liam  (22/09/2010)
 9  I think the question you raise is overriding, but I am not sure whether
10  technology is really the central point. A more general question could probably be
11  asked, and actually has been : are there more criminals today than 50 years ago,
12  or are we just better at detecting and counting torts and crimes? […] Maybe the
13  real question is what we want, how we conceive safety, what social and ethical
14  costs we are ready to pay when we think our safety is in jeopardy […] which
15  technology is best adapted to adress our goals? Is it biometrics? […] In the
16  movie, we see for instance that what makes the suspected man 'clean', is that he
17  is a european citizen with no criminal record […] Is that really the information
18  we need in order to increase safety? […] How is the fact of being a european
19  citizen, and yet how is biometrics technology, relevant to cope with the
20  terrorist threat? […] So the questions raised by biometric passports are not only
21  ethical, but one can also doubt their efficiency.
```

The main focus here is on the contribution of Liam in response to a relatively simple question posed by Kathryn who asks "if advanced biometrics has come about because of increase in 'evilness' of people, or […] we are able to see the 'evilness' […] because of the increase in technology" (lines 2-4). Liam begins by rephrasing the question in more general terms, doubting the centrality given to technology (*I am not sure*). "[A]re there more criminals […] or are we just better at detecting" (lines 11-12). But Liam also suggests a "real question" focused on "what we want, how we conceive safety, what social and ethical costs we are ready to pay when we think our safety is in jeopardy" (lines 12-14). This series of questions is followed by a different set of questions asking, "which technology is best adapted to adress our goals? Is it biometrics?" (lines 14-15).

At this juncture, Liam has crafted a line of reasoning which hones in on a specific target question: *can biometrics address our goals*? First, he asks the general question of *what we want*, then immediately embeds particular named phenomena, *safety*, *costs* and *jeopardy*, in a formulation of more specific questions in a sequel to the first. These phenomena are cast in terms of *conception* (safety), *social and ethical relevance* (costs) and *line of defence* (jeopardy). Another shift in reasoning is evident in the next move, where Liam has assumed that adequate resolution of the first series of questions will result in particular goals. So, which technology can best address these goals? Is it biometrics? At this juncture, the film is recruited. The targeted individual in the film passes the automated test because "he is a european citizen with no criminal record". Liam asks if this is "really the information we need in order to increase safety?". How is European citizenship and biometrics "relevant to cope with the terrorist threat?". The key claim in the concluding remark that follows is twofold. Casting doubt about biometric passports, "one can also doubt their efficiency", is arrived at by recruiting substantiating support from the film on the issue of EU citizenship, criminal record and biometric technologies in defence of a terrorist threat. Secondly, the assumption Liam makes—we arrive at specific goals by asking how we conceive of safety and what the social and ethical costs are of introducing biometric technologies in defence of safety—supports the remark that "questions raised by biometric passports are […] ethical". But these goals, the conception of safety and the costs are not further articulated. The point that biometric passports raise ethical questions

however, turn the attention back to the centrality given to technology and the target question whether biometrics can address our goals. We are not clear on what safety actually stands for, nor what the acceptable social and ethical costs are in its defence.

What we learn is that participants make considerable efforts to establish persuasive critiques which are aimed at computer systems, governance and costs, but also at reasoning itself, eg., the film babbles. We also learn that the actual labouring of reason and critique is particularly evident in the formulation of questions in which phenomena such as *machines*, *human life*, *rat race*, *politics* and *economy* (Jay) or *safety*, *costs* and *jeopardy* (Liam) are embedded and cast in ways that clarify the social and ethical relevance participants attach to them in relation to the imaginary presented in the film. The two contributions gathered here (D4.1.6 and D4.1.7) take radical turns in meaning-making, not only by adding new assumptions and raising questions. They labour to depict doubtful worlds. They make challenging claims and they labour to further give shape to what they see as important matters of social and ethical relevance.

Raising alarm, triggering discussion

If the film itself was designed to raise particular concerns or, as one participant put it, to `“push the hot buttons of 'privacy advocates,'”` (D4.1.1, line 22), it fails to do so. What raises alarm in reference to the film emerges in different guises. We observe how the film confirms to participants the assumption that biometric and other information technologies are necessary, that they are bound to occur because governments must be allowed to identify those who are a threat to ensure the continued safety and well-being of citizens. Uncertainties are primarily about who people are, the risks associated with letting them pass, the danger that someone wants to harm us, and the means of control are to track individuals and collect information, including biometrics. We also observe how the film confirms to participants the assumption that biometric technologies are positive, interesting and good to have. However, certainties and uncertainties about them are mitigated by casting doubt or asking questions. In particular, we see how questioning opens up avenues for further enquiry because it introduces – seeks to foreground and confirm – assumptions which are perceived as missing in the film or are mentioned specifically to complement or contradict it. We need personal control over privacy. The technology is not safe. It can be abused or it still needs figuring out. The law may not be adequately addressed, nor the EU objective of social inclusion. Uncertainties are related to safety, decision-making and operation. The risks are associated with potential identity theft and unfair exclusion. The danger is that potential problems and uses are not debated, and control is associated with the power to include and exclude, to control private information or someone else's identity. Finally, we observe how the film confirms to participants mistaken depictions of the world, depictions that do not adequately question computing systems, governance or the social and ethical costs we already pay in Western democracies for an obsolete socio-economic and political system. The critique is that typical questions of uncertainty, risk, danger and control never get at the “bigger”, the “right” and the “real” questions of what the world needs, what people want, why technology is central, what meanings are attached to safety, a good life, and so on.

We argue that world-making and meaning-making which is initiated in the film, is an ongoing labour of co-construction to which everyone who participated in this forum makes some contribution. New assumptions are introduced, reasoning is shifted, general and specific questions are asked and new claims are made. By co-construction, we do not mean that meaning-making is eventually put to rest or that imaginaries are neatly aligned. Rather, what we call the ethics of imaginaries and meaning-making is manifest in procedures that substantiate disunity and tension. The film indeed serves the stated purpose of *triggering* these procedures by performing

an imaginary to which a number of participants relate explicitly in one or another way while other contributions do not. How shall we manage illegal aliens or harmful individuals? Do governments have a duty to protect and by what means? How can we manage privacy, potential identity theft, abuse or information and computing systems more generally? What kind of politics and socio-economic systems do we put up with? Are we asking the right questions? But, as we now continue our analysis, we leave the film behind to explore ongoing contributions over three or so months.

2. Addressing the topics: Issues of ethical and social relevance taking shape

In this section, we explore the ways in which the focus issues were addressed and how they take shape: *social justice*, *surveillance and privacy*, and *trust in technology and in government*. There are questions of privacy and dignity. There are issues concerning minorities and majorities, types of individuals, and the role of the state as well as other matters of governance. There are questions raised about biometric systems and networked information technologies more generally, about realistic expectations and so forth. We observe that the focus topics overlap to some extent but, for the sake of clarity, we deal with each separately. The contributions we refer to and analyse demonstrate not only that participants have opinions, beliefs and points of view on these matters. They demonstrate continued struggle over meaning-making and world-making whereby concerns, claims and questions are articulated with reference to understanding or assumptions which are either explicitly explained or presupposed.

1) *Freedom, security and social justice*

Although issues of social justice are not explicitly debated in the forum, they are anchored in many of the contributions which touch on issues of fairness, state abuse, system errors, or the perceived necessity to apply biometrics 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. In the previous section, both Anna and Brian highlight the uncertainties, risks and dangers when “we” or governments do not know who individuals are and if they want to harm “us” (D4.1.1). Brian more specifically emphasises the danger to the group and the safety of citizens and Anna insists that biometric systems will be used wisely to make society as a whole more secure. But questions are also raised, whether biometrics for surveillance and security purposes will be justly applied and can actually deliver improved security. In the previous section, Ian draws attention to issues of justice regarding decisions on who can be within the security envelope (D4.1.5). Liam asks how we conceive of safety and what social or ethical costs we are willing to pay in exchange for security technologies (D4.1.7), and Jay turns attention to terrorists and security threats as symptomatic of the injustices of the dominant socio-economic system (D4.1.6).

One can argue that some of the contributions are markers of social paranoia, in particular, in relation to the question of individuals posing a threat to the group. Consider this debate:

Fragment: ***D4.1.8***

Charles
What or who is the problem here, individuals or the technology [...] Is the implications that technologies also create increasingly dangerous societies, and that, therefore, individuals must be kept in check by the state? this seems to me like a locked-in situation. Biometrics, in that scenario, emerges as a good tool for controlling individuals. But do you think technology can perform this role? Can we have automatised recognition/profiling of dangerous individuals without errors, on a significant scale, occurring?

Arnie
It is both the individual and the technology combined that pose the existencial threat to the group. Most high technology is dual-use. That is it can be used for great good or great evil. For instance, in the paper "The Darker Bioweapons Future," it is stated that the genomic revolution enables technology that can be used to cure some diseases that have plagued man, or used to create a disease worse than mankind has ever suffered.

Charles
But one question remains: is biometrics capable of perforimng the functions you describe, i.e. can dangerous individuals be detected, as implied by projects like Project Hostile Intent, FAST (http://en.wikipedia.org/wiki/Future_Attribute_Screening_Technology), or some projects presently being researched in the European Union?

Arnie
Biometrics, like any technology, is a tool. Specifically, biometrics uses charactoristics (i.e. measurements) to identify individuals. It can't be used to look inside their souls. Biometrics will no doubt be used as an electronic key, where an individual, once identified, will be let through closed doors they are deemed to deserve to enter. Furthermore, biometrics will be used to track the movements of individuals across the globe and through crowds. These functions will be necessary to control the population and ensure an orderly society.

While Charles is pushing the question whether biometrics can perform the role of detecting and controlling dangerous individuals, Arnie continues to depict the individual as a potential danger to the group, a danger to security and the state. He believes that biometrics will be used like an electronic key and that tracking the movements of individuals in crowds and on the move "will be necessary to control the population and ensure an orderly society" (lines 32-33). We also observe how this 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*. Consider these examples:

Fragment: ***D4.1.9***

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**.

Isobel
There will if course need to be more intrusive security for **those deemed high risk** […] We're talking about the path to a high technology society, which I think is worth the cost of some better **awareness by government of the activities of individuals**.

Jacques
I would like to remind you that **1 in 20 people (estimate) are psychopaths** [...]

```
15  it does mean that there is a significant number of people in our society that
16  have the emotional and psychological freedom to commit unspeakable crimes if
17  they choose to. As an example, the genomic revolution enables individuals to
18  construct highly contagious extremely lethal virus. A severe pandemic would
19  cause our civilization to collapse, killing billions. Don't believe me?  Check
20  out the paper "The Darker Bioweapons Future" written by the CIA (unclassified).
21  Don't underestimate the power of an individual even in this pre-high technology
22  society to destroy the group.  The power of the individual will only grow as our
23  technology becomes more advanced.
24
25  Kevin
26  I would think that the majority would want closer monitoring and control of
27  everyone so as to be protected from the minority.
```

Hillary does not believe that security systems can do the job of keeping *all* criminals at bay. "[H]ardcore criminals will always find a way to subvert any security system" (line 2). The best case scenario is that "minor criminals are stopped" (lines 3-4) and the worst case scenario that "innocent people suffer due to the enhanced security" (lines 4-5). Isobel takes for granted "more intrusive security for those deemed high risk" (line 8), which is only the cost of "better awareness by government of the activities of individuals" in a high technology society (lines 10-11). Jacques emphasises "that 1 in 20 people (estimate) are psychopaths" with "emotional and psychological freedom to commit unspeakable crimes" (lines 14 and 16). This statement is followed by the hypothetical scenario (for comparison) of an individual constructing a lethal virus. Jacques warns the reader: "Don't underestimate the power of an individual" (lines 20-21) which "will only grow as our technology becomes more advanced." (lines 22-23). Finally, Kevin thinks "that the majority would want closer monitoring and control of everyone so as to be protected from the minority" (lines 26-27).

All of these statements recruit proportion. Best and worst case scenarios are weighted against each other to casts doubt on the effectiveness of security systems. More intrusive security is associated with high-risk individuals who need to be detected and controlled by governments. The power of the individual correlates with advancing technologies, 5% of which are psychopaths and, finally, 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 the minority.

Recruiting proportion is not a particularly unusual or unique method of persuasion but what we observe is a dead-lock in reasoning about dangerous individuals. There is always a way to subvert a system, but we need the system to stop as many criminals as possible. The worst get off, everyone suffers but more security anyway. Individuals become more powerful as the technology gets more sophisticated, which calls for still more sophisticated technologies to stop the empowered individuals. The majority decides on a monitoring scheme of everyone without exception, in order to control poorly defined minorities. One can ask, with good reason, to what extent these depictions resonate with the current climate of securitisation which is already risking to criminalise any citizen to protect the freedoms of Western democracies, and to *keep us safe* (See D1.1; also Bigo and Tsoukala, 2006). Profiling and sorting out the dangerous or deviant draws attention to questions of inequalities, fairness and discrimination. These practices have strong implications for social justice, in particular, the insecurities that arise with respect to decisions on who is targeted and precisely for what reason, or what the unintended consequences could be. As Hillary suggests, "[a]t the worst innocent people suffer". But what we observe of notice in these contributions is evidence of social paranoia which begs the question of how this paranoia is cultivated and what the implications are for social justice.

2) *Surveillance and privacy*

The right to privacy continues to be high on the agenda of data protection and human rights advocates but the relevance of privacy is not always clear, nor what it actually stands for. When the question takes priority of who is a trusted traveller and who is a potential threat, high degree of privacy is no longer desirable (see Sutrop, 2010 on this issue). There is no definitive "right to privacy" either. For example, according to the EU Charter of Fundamental Rights, there is only "the right to respect for [...] private and family life, home and communications" (European Communities, 2007: Art. 7).

What counts as privacy is difficult to clarify except in reference to breach and what counts as breach varies significantly, i.e., the margin of appreciation.[5] It is therefore difficult to prevent breach with consistency across cultures and social activities. Privacy is also cast in terms of control, that persons have reasonable control over who can access them or information about them, what precisely is accessed and for what purposes. Otherwise, it is the duty of state agencies and constabularies, to protect persons and personal data from mishandling. Having control however, is increasingly 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 often retained.

What we learn from the forum supports these complications and demonstrates the extent to which the notion of privacy is anchored in concerns about respect, breach, control, trust, purpose or protection, i.e., to give privacy meaning and relevance. For example, Emilia's question in the previous section, if one could be *on* and *off* at will, does not clarify what counts as privacy (D4.1.3, lines 3-5). It is a concern about how to be in control of access to oneself which lends relevance to the notion of privacy. But, we also saw in fragment D4.1.1 that Brian does not buy into the idea that privacy is a concern in the use of biometric systems. Consider this contribution:

Fragment: ***D4.1.10***

```
1  Mina
2  My position is that privacy in a high technology society is of secondary concern
3  to the security of the group. Biometrics will enable us to closely scrutinize
4  individuals tagged for closer observation, and quickly identify the perpetrators
5  of crimes. Using the data from biometric observations, we will also be able to
6  analyse patterns of movement for criminal intent, and automatically more closely
7  scrutinize those individuals.
```

Mina's position is that privacy is secondary to security (lines 2-3). She downplays privacy to secure the group and casts no doubt on the ability of biometric technologies to achieve this. `"Biometrics will enable us […], quickly identify the perpetrators"` (lines 3-4), and `"we will […] analyse patterns […] and automatically more closely scrutinize"` (lines 5-7). As Mina articulates, biometric technologies are enabling in particular ways which make privacy a secondary issue. We can scrutinise, tag, identify, observe and analyse for the security of the group.

Giving away biometric information however, raised a number of questions such as how to strike balance between privacy and security, understanding the consequences of giving away this information or being free to decide whether to give it away, having some protection, and distinguishing between different purposes (government, workplace, business) for which the information is used:

5 "Margin of appreciation" is a guiding tool used by the European Court in Strasbourg to assess data uses or data protection directives against social-cultural sensibilities toward intrusion, what counts as private, and so on.

Fragment: ***D4.1.11***

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?**

Noam articulates what he is important. "I think everyday we release a lot […] The import[ant] thing is to know what are the consequences […] and being free to decide" (lines 2-4). He continues along these lines, that "people should be informed about" the information they are giving away, as well as the "impacts in terms of privacy and security", who is delivering these services and when the information is used (lines 4-7). Then he raises a question. "Probably […] security could improve" but does "the increase in security compensates the privacy losses?" (lines 9-11).

Issues of consequence, protection and purpose also came up in exchange between participants who were sharing experiences that draw attention to the legal ramifications when implementing biometric check-in and authentication systems.

Fragment: ***D4.1.12***

Omar
At my workplace there is fingerprint system to register the service hours. […] When I did the procedure to introduce my biometric data in the system in the first day of work I did not question if it was a legal thing to do or if it could be privacy issue. I have to admit that even if probably is not a legal system, I do not feel that the fact that they have this data from me can be use against me. But I know that since the system is not official and I never made a confidentiality agreement related with my biometric data with the company, in a conspiration scenario,....I could have problems

Patrick
I have something of the same experience: first, in my gym biometrics appeared as the main check-in authentication mechanism (I give my thumb fingerprint and a number). I am not particularly worried about this: first, the thumb is not used by the "main" systems, such as at airports and the like; second, I know that the system they use is probably not interoperable with other systems and so my biometric will be of little use outside that context. What I did not like, however, was that the system was introduced seemingly without asking or informing anybody about possible insecurities of the system/possible privacy problems or potential (however small) for identity theft […] How was the situation at your workplace: did biometrics replace another system for checking in and out, or did it imply tighter control with workers? Why did they need it, are you working at a high-security facility?

Omar
I work in a University research institute...with no hight security or hight confidentiality research. Before there was no control on checking in or out. The biometric system was the first system to be implemented. We are more than 200 people so, is difficult to control presences, and I know there where some people abusing .... Nevertheless.....people should be informed about the issues related with the biometric information, and probably legally a data confidentiality should be signed. Do you know if these type of systems can be implemented without special authorization?

Both Omar and Patrick claim not to be worried about giving away their data in the workplace and the gym respectively. "I do not feel that the fact that they have this data from me can be use against me" (lines 5-6) and "I am not particularly worried about this" (line 14). Omar does not substantiate his claim, however, Patrick does in relation to the gym. "[T]he thumb is not used by the "main" systems, such as at airports" and "the system they use is probably not interoperable with other systems" (lines 14-16). Patrick also raises a concern, that "the system [in the gym] was introduced seemingly without asking or informing anybody" (lines 18-19), and he questions the security of the system as well as of the data, i.e., the "potential (however small) for identity theft" (line 20). But Omar has drawn attention to legality, "I did not question if it was a legal thing to do" (lines 4-5), and privacy, "or if it could be privacy issue". He knows this is an unofficial system and "I never made a confidentiality agreement […] with the company […] I could have problems" (lines 7-9).

What we learn from this exchange supports the sentiments expressed in fragment D4.1.11, that people should be informed, but it addresses more specifically questions of legality, officialness and authorisation. Patrick asks about Omar's workplace, why the system was installed, and so on, and Omar briefly explains that it was not a high security institute or confidential research, but it was hard to oversee human presence and the system was introduced for that purpose (lines 26-30). Omar aligns with Patrick's concern, "people should be informed" (line 30), but he raises the point again about legality and confidentiality agreements, asking: "Do you know if these type of systems can be implemented without special authorization?" (lines 31-33). This question brings out the role of Data Protection Authorities (DPA) in a follow-up comment by Patrick and, thereby, anchors privacy specifically in official measures for data protection (lines 5, 7, 31-33).

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:

Fragment: ***D4.1.13***

```
 1  Quine
 2  For me it means being able to move freely, especially in public spaces (online
 3  and offline). I believe public spaces are threatened and in need of being
 4  defended. This also goes for ICCTV and similar applications.
 5
 6
 7  Regina
 8  Very complex topic. [… ] it highly depends which world we have in mind. In
 9  current world, where everything has a price tag and is for sale, I am afraid that
10  aggressive implementation of biometric technologies (not just passports) would
11  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.

Again, the facilitator asks what privacy means, this time under the subject, "[w]hat does privacy mean for you?". We find that some participants, although seemingly responding to the question, quickly shift the attention to much broader concerns about the economic and political climate. There are particular connections made here between trust, governments, elites, and the need for privacy.

Fragment: ***D4.1.14***

```
 1  The main problem is lack of trust. Lack of trust is particularly a problem
 2  regarding Governments. If we could trust Governments and if we could trust
 3  people in our communities then we would have little need for privacy.
 4
 5  PRIVACY IS CRUCIAL AND PRIVACY FROM GOVERNMENTS IS THE MOST NEEDED PRIVACY
 6
 7  The whole concept of privacy is about State/Government control. Privacy is one
 8  of the many ramifications arising from "The Power Elite" controlling "The
 9  Masses". […] This capitalist greed creates the need for privacy. Inequality
10  creates the need for privacy. Capitalist selfishness, perpetuated by The Power
11  Elite, creates the need for privacy .
12
13  Privacy is the restriction of information from enemies/hostiles. Between family
14  and friends there is little need for privacy because they are trusted.
```

Two statements are noteworthy. The first is an *if* clause stating that "we would have little need for privacy" *if* governments and people around us could be trusted (lines 2-3). The other states that "[b]etween family and friends there is little need for privacy because they are trusted." (lines 13-14). In other words, outside our closest circle of intimate and familial relations we can have no trust whereas inside our closest circle we can. Put this way, the need for privacy is anchored in *lack of trust*, although it remains elusive what "trust" and "little need for privacy" could actually stand for in everyday affairs.

We see that repeated probes for the meaning of privacy only illustrate that the notion is problematic on its own. The facilitator resorts to additional questions such as breach when one's private life is made public or when one knows or suspects that one is being watched. He resorts to questions about giving away biometric information and to what extent such information can be used by governments or businesses. The privacy-related issues that emerge, mention greed, power, harassment, theft, freedom of movement, and a range of concerns relating to agreement. For example, Omar states twice his concern about confidentiality both of which situate the notion of privacy and data protection in reference to officials or formal settings where two or more parties have access to personal information. Noam, Omar and Patrick argue that people should be informed about the data they give away about themselves, what can be done with it, by whom, and so on (D4.1.12). There should be an agreement, and there are questions of legality and authorisation. Taken together, these contributions all raise privacy-related matters in the sense that there is considerable uneasiness among participants over the uncertainties about personal information that *can* be collected and *could* be used. Being *informed* and having *protection* is, however, perceived as one way of overcoming such uncertainties.

3) *Trust in technology and government*

The questions the facilitator asks about issuing biometrics data, their collection and uses, are answered more clearly than the question about the meaning of privacy:

Fragment: ***D4.1.15***

```
 1  Siv
 2  Is it ok for you that you give biometric data to governments any time a police
 3  officer request it?
 4  Under strictly defined circumstances: yes. That is, only in order to confirm the
 5  authenticity of the documents I'm already using. If it in any sense implies any
 6  kind of investingation by defalut, automated suspicion and investigation so to
 7  speak, I am against it.
 8
 9  Is it ok for you that governments exchange this information?
10  No. Only, as I said, in the case of investigations of already known criminals.
11
12  Is it ok that private companies collect this data?
13  NO!
14
15  Trevor
16  is it ok for you that you give biometric data to governments any time a police
17  officer request it?
18  I dont see a problem with that if biometric data contains only most basic
19  informations that identify me as person X. Police officer also has a number ;)
20
21  is it ok for you that governments exchange this information? is it ok that
22  private companies collect this data?
23  Same as first answer.
```

Siv and Trevor both give succinct answers, although, their beliefs are not the same. Siv's opinion is that a policy officer can only use her biometrics to `"confirm the authenticity of the documents I'm already using"` (lines 4-5), while Trevor states that a police officer can only use the simplest biometrics to `"identify me as person X"` (lines 18-19). Siv claims that governments can only exchange biometric information when investigating `"already known criminals"` (line 10) and that private companies cannot collect biometrics at all, while Trevor answers the second and third question, `"[s]ame as first answer"` (line 23), i.e. only the simplest biometrics can be exchanged by governments or collected by private companies.

What is problematic about these contributions is that Siv and Trevor give no explanations for why they have come to these particular conclusions, i.e., there are no lines of reasoning to explore. What we learn however, is that they articulate two privacy-related issues which are matters of privacy protection and privacy enhancement. Siv wants to minimise purposes for using biometrics while Trevor wants to minimise the amount of biometric information in use.

On the issue of centralised databases, we see questions raised about synergies and interoperability between EU databases. In a nutshell, this means systematic exchange of data and the sharing of information and knowledge, achieved by organising and streamlining protocols, practices and connectivity for better availability of data to various EU agencies and beyond.

Fragment: ***D4.1.16***

```
1  Yvonne
2  One of the most contentious issues relating to biometrics in the European Union,
3  to take this as an example, has been the issue of centralised registries
4  (www.statewatch.org/analyses/no-45-sisII-analysis-may05.pdf). The problem is: if
5  such registries are dropped, will it not be difficult to compare biometric
```

```
 6  templates across jurisdictions? If my passport is falsified, and the only check
 7  is between the template stored on my passport and my biometrics (fingerprints
 8  and face), then the border guard, or whoever wants to check up on me doesn't
 9  have a reference. Hence, if I get this right, much of the added value is lost
10  without the centralised database.
```

Yvonne has actually put a finger here on persistent tensions between those who believe that centralisation is of the essence to maximise the utility of these technologies, and those who resist centralisation precisely to minimise certain kinds of utilities, for example, data exchanges between agencies and jurisdictions which involves the comparison of templates and checks against issued IDs and additional information on the individual. These are well known issues in professional and policy discourse on biometric systems which relate to questions about centralised registries, i.e., more specifically, if we can separate meaningful utilisation of biometrics from centralisation. But if this is the way the new databases are heading, do privacy and data protection directives provide some protection or are they mainly smokescreens? Can we trust governing bodies with these systems? What about 'function creep', when data collected for one purpose is at a future date used for another purpose? Consider this example:

Fragment: ***D4.1.17***

```
 1  Warner
 2  Biometrics should be used to verify documents only, and not stored in centalised
 3  registries, except in very limited cases, such as already existing fingerprint
 4  registries of KNOWN criminals. It should by no means be used for investigative
 5  purposes or for tracking people's movements; this is my gut feeling.
```

Warner *tells* the reader what the technologies should be used for, a remark which resonates with the privacy-enhancing concerns raised in fragment D4.1.15, i.e., to severely limit both purposes for use and data in use. The option which is explored here is a check between a template embedded in an ID carried by a person and that person's biometrics taken on the spot without the need to aggregate further information. This option has been argued for, to keep the utility of these technologies as close as possible to the person in question, rather than allowing the data to take on a life of their own in registries with distributed access and unforeseeable future uses with unintended consequences:

Fragment: ***D4.1.18***

```
 1  Zygmunt
 2  consider the context that brought us to the present stage of implementation. We
 3  know that the potential for misuse is great, especially so when access is
 4  provided to an increased number of authorities in Schengen and beyond. The chain
 5  is not stronger than the weakest link, and it only takes one corrupt officer to
 6  sell or misuse my biometrics, or additional information. And how big will not
 7  that chain of officers be when systems VIS and SIS II etc. are up and running?
 8  The whole context is problematic, introducing biometrics to fight terrorism,
 9  mainly under pressure from the US. But can the technology serve this purpose? As
10  pointed out by [another participant], a number of technical problems are not
11  sorted out (can they be?), but political pressures drive up the speed.
```

Here we learn how Zygmunt takes into account potential misuse of biometrics, albeit, not misuse instigated by politicians, policy makes, industry or government agencies as such, but individuals who handle these data on an everyday basis. The claim here is that a chain of

dishonest officers can only grow as new systems are implemented and the access to the data distributed even further. We also learn how Zygmunt takes into account the political pressures to implement these new, larger and more accessible systems which resonates with an observation about EU practices in the previous section (fragm. D4.1.5), and contributions stating that technical problems are yet unresolved (D4.1.4; D4.1.6; D4.1.8). What we observe is an awareness of current trends and immediate future plans for biometric systems within the EU and beyond, however, with unresolved questions about the extent of their potential and acceptable utility. What Zygmunt draws attention to specifically is the extent to which such large-scale sociotechnical operations, involving officers and a range of occupational interception, may encourage or be vulnerable to dishonest or disruptive practices.

As we learned in the previous section, the short film raises issues of whether governments can be trusted. This question continues to take shape over time in the forum, as we saw for example in relation to privacy (D4.1.14) and on the question of issuing biometric data (D4.1.15). There is also evidence of assumptions about tension and threat between individuals and the state, for example, we observe a comment with an all-capitalised statement, `"THE PROBLEM IS GOVERNMENTS"`, followed by, `"[t]hey should have less power over people, not more. We must restrict the information Governments collate about people"` or `"[t]ime and time again Governments demonstrate how they are willing to commit atrocities in the name of peace, freedom, democracy, and security."` One Technolife researcher posed the question of state power in relation to the issue of distributed versus centralised information systems:

Fragment: ***D4.1.19***

Esther
Many Western states have no centralised database on all citizens. Identifiable information is distributed and checked against photo-id cards, signatures, pin codes, etc., and now biometrics in some cases. There are big fears about centralising information on individuals. Individual freedom against "the state" and state power--sort of thing, say, if we suddenly had a nasty government.

Fanny
I dont share paranoia of *some* western countries about central registers. If someone wants to kill me for example, he/she doesn't need sophisticated biometric registry to track me down and eliminate me […]. To rob anyone, they dont need tech either as they already control money supply through central banks. Do they need secret biometric data to publicly discredit or demonize someone? We dont need biometrics to control modern slaves as 20th century made a new kind of slave that promotes and protects its own submission proudly and stubbornly. We dont need central register of any kind to poison vast majority through public water treatment facilities. Why would nasty government need biometric databases when they can always bribe or force bureaucrats working on already existing paper documents.

Fanny does not refute that there are tensions between individuals and the state or "others" with means to do harm. What Fanny is refuting is the need for `"sophisticated biometric registry […] secret biometric data"` or `"central register of any kind"` to eliminate people, discredit or demonise, control money supply, poison or enslave a population. `"Why would nasty government need biometric databases"`. Whether or not the state or a powerful "other" can do massive harm to individuals without centralised registries will not be assessed here. But Fanny's argument does not take into account the actual historical uses of centralised registers, precisely, to track down and do harm to individuals listed on the registers as of one or another sort. A comment was made by one participant about the Dutch experience of records on individuals during WW2 and, consequently, that race can no longer be recorded in Dutch registries. Another participant expanded on that comment in the following:

Fragment: ***D4.1.20***

```
 1  Agnes
 2  I do think it is important to remember these historical examples: If national
 3  registries and ID cards can be used for purposes of genocide; can this potential
 4  not be enhanced by "direct online" access to individuals and groups? (what is
 5  especially problematic here is the subsumption of indivduals under certain
 6  groups. An individual can, in most cases be seen as unique, also through his or
 7  her fingerprint, face etc. But group identity is always also a social construct,
 8  and so is likely to contain also strong power interests, or distinctions that
 9  are made more or less by random. Thus it is all the "extra" information that is
10  heaped onto individuals, for instance in terms of ethnic information, as in soft
11  biometrics, that can be problematic).
```

What we observe here is that further developments on the issue of trust in governments and governing practices shift the attention toward the safety of groups, but Agnes only touches on the issue of *social sorting* rather than perceiving strictly of government as a danger to the individual. In doing that, Agnes also draws attention to measures already in place (including biometric technologies) to sort people socially into groups, and the interest groups who seek to further their purposes with respect to certain categories of individuals, i.e., the `“subsumption of indivduals under certain groups […] strong power interests, or distinctions that are made more or less by random”` and `“all the 'extra' information that is heaped onto individuals”`. (lines 5-10).

Ethics of biometric technologies

It is not our intention to assess the value of various claims made by participants or to moralise about their opinions, beliefs, attitudes or sentiments. Rather, the purpose of the analysis in this report has been to explore the ways in which the focus issues emerge in response to the film and to further explore the variety of depictions or imaginaries participants contribute, as well as the tensions we observe in their efforts to give matters of concern both meaning and relevance.

Participants contribute a rich source of data in response to the film: in the way in which they articulate certainties about biometric technologies or mitigate them, ask questions and push them or, otherwise, perform substantial critiques of dominant socio-technical imaginaries of operating biometric and other information systems. The topics that take shape pertain to implications that are of interest or concern. Profiling and social sorting, detection of suspicious behaviours and terrorist threats, more intrusive security associated with high-risk individuals, are but a few examples of activities associated with the use of biometric technologies, for which there are consequences participants have issues with. They question whether we actually have protection of rights and liberties. They question the desirability of privacy. They question if we can fully understand the consequences of issuing biometric data or if we can clearly distinguish between different purposes for which biometric technologies are operated. Questions of trust in these technologies, in government agencies and corporate enterprise are very prominent in the exchange on these topics.

Importantly, many depictions and issues that are raised take their shape interactionally, either between participants themselves or in response to probes from the facilitator. Thus, participating in the forum on biometric technologies is social participation in the sense that technologies of articulation, persuasion and mediation find expression in communicating with others, exchanging views, agreeing and disagreeing, but most significantly they find expression in ongoing efforts to fine tune the assumptions on which arguments are developed, matters explained, claims made,

challenges posed, and so on. What the forum does not accomplish however, is to draw together collective opinions, concerns and attitudes, belonging to particular identifiable social groups who, *as groups*, have stake in current affairs and future development. This is unfortunate given the objective of the Technolife consortium to address ethical considerations at the meso-level. We observe persistent lack of signification by participants, of belonging to a particular group. One can also argue that most of the issues addressed in the forum are well known in the circles of academics and policy-makers which begs the question of what the Technolife forum can add to ethical debates on biometric technologies. We observe that discussions on same or similar topics can be found in online blogs around the same time, but what we also observe is that online communities, including the Technolife forum, can serve as outlets for political and socio-economic dispositions which have considerable currency but are ideological "no-go-zones" in official democratic deliberation. Participants reframe completely what the key problems are and which issues need discussion and debate. With respect to the deployment of biometric technologies, the sanity of the dominant security rationale is subject to considerable doubt. The question is raised in earnest, if Western democracies use biometrics to secure themselves from so-called enemies of democracy, whose grievances are merely the symptoms of "us" imposing on "them" oppressive non-democratic socio-economic regimes to support global capitalist and militarist agendas which are essentially indefensible and unsustainable. They also find an outlet in the forum to express sentiments, strongly signalling a cultivation of social paranoia in the current political climate, grappling with citizenship, transnational development and securitization. These dispositions, and the ways in which they reframe problems and debates, are likely to be ignored or played down in the foreseeable future.

Bibliography

Bigo, D. and Tsoukala, A. (2006). *Illiberal Practices of Liberal Regimes: The (in)Security Games*. Paris: L'Harmattan.

Council of the European Union (2009). *The Stockholm Programme - An open and secure Europe serving and protecting the citizens*. EU Presidency to General Affairs Council/European Council (Brussels 2.12.2009). http://www.se2009.eu/polopoly_fs/1.26419!menu/standard/file/Klar_Stockholmsprogram.pdf

Council of the European Union (2004). *The Hague Programme : strengthening freedom, security and justice in the European Union*. EU General Secretariat to Delegations (Brussels 13.12.2004). http://ec.europa.eu/justice_home/doc_centre/doc/hague_programme_en.pdf

European Commission (2004). *Area of Freedom, Security and Justice: Assessment of the Tampere programme and future orientations*. Commission of the European Communities to the Council and the European Parliament (Brussels, 2.6.2004). http://ec.europa.eu/justice_home/doc_centre/intro/docs/bilan_tampere_en.pdf

European Communities (2007). *Charter of Fundamental Rights of the European Union*. Official Journal C 303/01. http://eur-lex.europa.eu/en/treaties/dat/32007X1214/htm/C2007303EN.01000101.htm

European Parliament (1999). *Tampere European Council, 15 and 16 October 1999 : Presidency Conclusions*. Council of the European Union. http://www.europarl.europa.eu/summits/tam_en.htm

Jasanoff, S. (2003). Technologies of humility: Citizen participation in governing science. *Kluwer Academic Publishers* **41**(3). pp. 223-44.

Rommetveit, K., Gunnarsdóttir, K., Jepsen, K. S., et al. (In Press). The TECHNOLIFE Project:

An experimental approach to new ethical frameworks for emerging science and technology. *International Journal of Sustainable Development*.
Sutrop, M. (2010). Ethical Issues in Governing Biometric Technologies. In A. Kumar and D. Zhang (eds) *Lecture Notes in Computer Science (Vol. 6005)*. Springer. pp. 102-14.
Wynne, B. (1992). Misunderstood misunderstanding: social identities and public uptake of science. *Public Understanding of Science* **1**(3). pp. 281-304.
Wynne, B. (1988). Unruly Technology: Practical Rules, Impractical Discourses and Public Understanding. *Social Studies of Science* **18**(1). pp. 147-67.

Bibliography