Article

'My fingerprint on Osama's cup'. On objectivity and the role of the fictive regarding the acceptance of a biometric technology

Susanne Krasmann

University of Hamburg, Germany.
susanne.krasmann@uni-hamburg.de

Sylvia Kühne

University of Hamburg, Germany.
sylvia.kuehne@wiso.uni-hamburg.de

Abstract

In inquiring about the social acceptance of the digital fingerprint during our research, we discovered the crucial role the fictive plays in our interviewees' experience and assessment of control and security technology. Social acceptance is thus a heterogeneous phenomenon, not only because it depends on the situational features of dealing with the technology, but also, notably, because facts and fiction intermingle, sometimes indistinctly, within the discourses on surveillance and security. Mistrust in the technology tends to feed on fictive imageries, while at the same time resting on an unwavering belief in the objectivity of fingerprint data, presumably a clearly decipherable and reliable form of forensic proof. Against this backdrop, the article seeks to investigate the fictive's critical role in countering security technologies.

1. Introduction: definite data and indefinite imagination

J: [...] and then the police ask, you have applied for an ID with a fingerprint, and they then have your fingerprint—and if through some coincidence I've grabbed hold of a coffee cup, the police hold me for observation, take the mug with my fingerprint, and can prove that it's me.

A: Well, if I'm somewhere like the United States and have to give my fingerprint, it can then end up in some kind of database, and if I'm travelling around and somewhere I grabbed hold of a glass where a potential Al Qaeda guy might've been sitting nearby drinking a coffee—I can imagine that I would then have all kinds of problems.

These two quotes from a study we have conducted on the social acceptance of fingerprinting are exemplary, especially with regard to two motives that have repeatedly come up in our interviews. On the one hand, we encountered what might be called a fear of loss: as soon as a fingerprint is submitted to a governmental authority, it may obtain a life of its own. The person no longer has control over her own fingerprint. The fingerprint itself, on the other hand, is deemed by our interviewees to be unambiguous and objective. There is no doubt that once a fingerprint is found somewhere as a left trace, it will speak the truth. That *my* fingerprint is at issue, proving that I was *there*, i.e. at the crime scene in question, will be undeniable. The fingerprint verifies 'that it's me'. The fear of unnoticeably being profiled and (falsely) identified, which is sometimes encouraged by strong fictive imageries, rests upon a belief in the objectivity of the fingerprint. This deep-seated belief in the irrefutability and impartiality of automated

Krasmann, S. and S. Kühne. 2014. 'My fingerprint on Osama's cup'. On objectivity and the role of the fictive regarding the acceptance of a biometric technology. *Surveillance & Society* 12(1): 1-14.
<http://www.surveillance-and-society.org> | ISSN: 1477-7487

© The author(s), 2014 | Licensed to the Surveillance Studies Network under a [Creative Commons Attribution Non-Commercial No Derivatives license](https://creativecommons.org/licenses/by-nc-nd/4.0/).

control technologies in general is clearly tied to the notion of an impermeable, and inscrutable, world of data collection and data mining that is experienced by ordinary people in unforeseeable control interventions.

This article will discuss this intersection of information, or knowledge and presumed facts, about control technologies on the one hand, and imaginations and visions of control on the other. To capture the significance of this intersection, we draw on the notion of the fictive used in literary studies (Iser 1993). The fictive is neither real nor unreal or illusory. As a form of 'doubled reality', it does not compete with, but adds to the 'real reality' and, as a mode of deciphering reality, it is at the same time no less real for us (Esposito 2007: 31).¹ Nonetheless, there is more than simply interpretative types and schemes in a social constructivist sense at play here (Keller 2005). For one thing, the notion of the fictive underscores that imagination and the imaginary, which go beyond the grasp of linguistic hermeneutics, are vital elements of our creation of reality. For another, the fictive is a relational concept: it resides between and interconnects reality and the imaginary. It is, in this sense, entirely performative, a form of creating reality by determining the imaginary.

Fictional imageries that are produced and reproduced discursively are central to the discourse on surveillance technologies in general and the digital fingerprint in particular. Although in principle still distinguishable from other realms of reality, fictional references, like the allusions to Big Brother and *1984* that are drawn from movies or literature, intermingle indistinguishably in our modes of deciphering reality. They are, in Charles Taylor's sense (2002), part of our 'social imaginaries' which exceed the individual imagination. Social imaginaries should not be confused with the notion of 'collective conscience', the latter of which suggests the existence of a homogenous and socially shared body of meanings. Social imaginaries are neither ideological nor habitualised, neither 'explicit doctrine' nor implicitly 'embodied knowledge' (Calhoun 2004: 377). They are pre-verbal in that they do not fully assume any kind of concrete meaning. Imaginaries are, in this sense, indefinite, but also have an unlimited potential to grasp, construct and constitute our social world through imagination (see Taylor 2002: 106-7). Whereas Taylor refers rather to political notions, such as the common idea of public protest and democracy that leads people to take to the streets in the first place, our focus here will be on the fictive that articulates itself in our perceptions, imagination and argumentation.

By relating our interviewees' statements to argumentative figures of the public affirmative as well as the critical discourse, our analysis aims to grasp these different modes of accessing reality and the attendant truth effects. In the first section, we provide a brief overview of the politics of the biometric fingerprint and its introduction in Germany after the 9/11 terror attacks as a feature of the passport and identity card. This overview will be supplemented with core arguments and narratives of the affirmative, as well as the critical discourse on this security technology in particular and surveillance in general.² Drawing on our own empirical research,³ in the following section we discuss the role, as echoed by our interviewees, of fiction and imagination within the discourse on surveillance and security. In the final section, we

¹ Alluding to Niklas Luhmann's observation of differentiation processes by social systems, Esposito (2007) uses this term to capture a kind of second-order that schemes of probability calculation and risk attribution produce.

² Although the affirmative discourse is mainly supported by public authorities and politicians arguing in favour of the introduction of biometric technology, it is not reducible to the 'official discourse' (Bourdieu 1992: 150). Similarly, the critical discourse is not reserved for civil rights organisations, for example, but may also be supported by oppositional politicians, the commissioner for data protection, etc.

³ Apart from analysing 177 articles from 2001 to 2010 in German newspapers and journals on the introduction of fingerprints in German passports and IDs, the main basis of our research on 'Biometrics as "Soft Surveillance"'. On the acceptance of fingerprints' (funded by the German Research Foundation) were observations followed by about 60 guided qualitative interviews that we conducted in different contexts concerning a rather voluntary use of fingerprint technology (e.g. as a tool of verification for payment procedures, instead of the debit card in supermarkets or as a device for access procedures in video rental stores).

demonstrate that engaging in the analysis of the fictive allows us to better comprehend the truth effects of the discourses on security and surveillance and how they may shape social acceptance.⁴

2. Fingerprint technology in the German discourse—a brief overview

The history of fingerprint technology dates to the 19th century,⁵ when it was imported from Asia to Europe and initially employed for administrative purposes (Cole 2001). As a police technology, manual fingerprint analysis in Germany has been a valued tool of criminalistics since as early as 1903. In 1993, it was introduced as an automated procedure for supporting legal prosecutions. It is only with the development of digitalised information technologies that fingerprinting could become a pervasive technical device, though during the 1990s it was still mostly only applied in particular contexts like access control in high security areas or authorisation in e-commerce. According to an official study on behalf of the German Parliament, even at the turn of the millennium, the capability and reliability of biometric technologies were still considered largely unproven (Petermann and Sauter 2002). This assessment apparently changed completely with the 9/11 terror attacks, which immediately prompted the then German Minister of the Interior, Otto Schily (2004), to require that digital fingerprinting be used in identity documents and that related data be gathered and interconnected. In fact, the minister could rest assured that the political-legal foundation had already been laid for his proposal. A discourse on migration, organised crime and transnational terrorism problems led to the endeavour to establish biometric data networks on a European level for containing 'insecure identities' and uncontrollable migration. In 2000, the Council of Europe decided to implement the European Dactylographic System (EURODAC) for the purpose of regulating asylum procedures among EU member states, and, in 2004, it established the Visa Information System (VIS) that would come to be one of the EU's most comprehensive automated biometric databases.⁶ From 2008, access to and comparison of fingerprint data by member states' law enforcement authorities and Europol was regulated by a variety of proposals of the European Parliament and the Council.⁷ Within this context, the requirement of the US to make biometric data in passports obligatory was only one catalyst for the development and spread of the technology in Europe. In Germany, digital fingerprinting was introduced for the passport in 2007 and for the ID in 2010, on an optional basis. What was once promoted as a technology for law enforcement purposes and border control became, after September 2011, an obligatory electronic procedure for non-EU citizens to acquire legal status ('electronic residence permit') and eventually a pervasive feature for every citizen's identity documents.⁸

There is, however, a decisive difference between the police and the visa databases (AFIS and VIS), on the one hand, and the common use of biometric data in identity documents, on the other. Whereas in the former case fingerprint data are stored in a central base and thus are permanently available for data collation, in the latter case they are currently saved on the respective RFID chip of the identity document and only readable by designated authorities like the police, customs and the tax office. Nevertheless, the options for extending the application field of fingerprints in identity documents, from verification to

⁴ Since our aim is to make a theoretical claim about the role of the fictive within the discourse on surveillance and security, rather than presenting the final findings of our research, the empirical material will be used for illustrative purposes.

⁵ Here, we refer to its first systematic use in the context of administration and identification systems, even though findings of fingerprints on ancient pottery imply that they have been used for more than 2000 years to verify authorship or identity (Cole 2001).

⁶ See the decisions EC No. 2725/2000 and 2004/512/EC.

⁷ See, for example, the amended proposal of 2012: 2008/0242 (COD).

⁸ Law on the adaptation of German Law on Council Regulation (EC) No 380/2008 of 17 April 2008 amending Regulation (EC) No 1030/2002 laying down a uniform format for residence permits for third-country nationals (12 April 2011).

identification, were repeatedly discussed until 2007.⁹ Hence, from the outset, the German Federal Commissioner for Data Protection and Freedom of Information cautioned that storing fingerprints—for instance, in decentralised databases like local residents' registration offices—would be easy to do due to indeterminate legal regulations.¹⁰ It was argued that without storage and police having access to, or at least being able to match, fingerprints in IDs using centralised databases like AFIS, recording fingerprints would be useless. Moreover, apart from the concern of identities being established through the technology as a means of prosecution—as one parliamentarian put it: 'if a criminal is caught, it is ultimately a good thing'¹¹—the benefit or even necessity of digital fingerprint devices for securing identity documents was put into doubt.¹² Indeed, Germany's ID's were already ranked among the most secure.

Against this backdrop, the affirmative discursive strategy sought to foster acceptance of the digital fingerprint as part of identity documents, with arguments revolving around issues of security, safety and convenience. One of the initial and main arguments suggested that the biometric passport and national identity schemes were necessary in the context of law enforcement and border control, namely, for determining suspects and distinguishing legal from illegal migrants (Klein 2011). So far, the fingerprint has been presented as the final security linkage between a person and her identity documents, and protection from 'identity theft' continues to figure as one of the key features of the debate: the device prevents terrorists from using fake or stolen IDs and, moreover, citizens are protected from possible routine fraud in the case of losing an ID.¹³ Nonetheless, it was only with regard to the passport that the digital fingerprint was praised as an essential tool for securing a person's identification. The main promise of the new ID, by contrast, was to facilitate verification in the context of new online services on the internet (for example, for e-government purposes), independently of the optional fingerprint. Given their concern with security and safety, these differentiations were rather insignificant to our interviewees.

Consequently, the fingerprint is presented as a privacy enhancing technology: not only is the personal marker secured through digitalisation and encryption, and in this sense 'hidden' in the RFID chip, but so are the document—along with the personal data on it—and the person's mobility. Furthermore, (border-) control procedures are said to be accomplished more safely and also more swiftly, since the identity document is endowed with a unique attribute.¹⁴ While the first lines of argument were echoed by our interviewees, the latter, although much emphasised and even part of public campaigns, played almost no role for them. Instead, as we will see, ideas predominated of various types of non-transparent control and surveillance.

In contrast to the affirmative discourse, civil rights organisations critically focus on the vast range of control options and challenge the argument of the largely discriminate and safe use of the data. For them, biometric data are more or less like personal data—a question of surveillance instead of security. Concern is raised with regard to what academic literature calls 'function creep', that is, either the unintended or

⁹ The Amendment to the Passport Act (24 May 2007) and the Amendment to the Identity Card Act (18 June 2009) explicitly prohibit storing fingerprints in centralized databases. The Federal Government specified the matching procedure of fingerprints to be a 1:1 (person-passport/ID) verification, and denied the possibility of identification on the basis of data base matching procedures (Federal Governments counterstatement to the Federal Councils statement on the Draft of the Passport Act, 28 February 2007). Biometric photos, however, are stored at decentralized data bases at a person's local registration offices and have in fact been made accessible to the police. But, as our research revealed, media coverage and interviewees often confuse this with information on data storage.

¹⁰ See, for example, the 19th Annual Report 2001 and 2002 of the Federal Commissioner for Data Protection and Freedom of Information, Bundestag printed paper 15/888, 7 May 2003, p.22.

¹¹ Wolfgang Freiherr von Stetten, Bundestag printed matter 14/192, 11 October 2001, p. 18713.

¹² See, for example, Bundestag printed matter 16/5507, 29 May 2007, and Bundestag printed matter 16/7073, 12 November 2007.

¹³ See, for example, Federal Printing Office (Bundesdruckerei) (2013); Federal Ministry of the Interior (2013).

¹⁴ See, for example, Germany's high-tech industry lobby *Bitkom* 2008.

unauthorised use of collected data (Mordini 2009) or the retrospective detection of further fields of application and legalisation. Civil rights organisations as well as academia are both wary that what is assumed to be technically possible could be realised and retrospectively legalised any time in cases of purported exigencies. Recent developments appear to have raised these concerns. The EURODAC database, for example, once established to control 'visa shopping' (European Commission 2005), is now in the process of also being made accessible to national security authorities and thus for law enforcement purposes.¹⁵ Critics warn that this might also happen one day to the biometric data on everyone's passport. With this eventuality becoming a pivotal political concern, the 'transparent citizen', a common metaphor in the German context, makes her appearance within the critical debate.¹⁶ Finding its blueprint in George Orwell's *1984*, it may be read as a complementary figure to an omniscient 'big brother'.¹⁷ Still, while Orwell's concern is particularly with 'the forces of oppressive authority', operating in *1984* through the imposition of the homogenising language, 'Newspeak' (Matos 2012: 13), the 'transparent citizen' represents rather an abstract and technologically driven threat to privacy in an 'eerie world of data' and governmental surveillance, devoid of a vision of a singular sovereign overlooking everything (Boeing 2006). The problem with the digital fingerprint is its pervasiveness and consequently the opportunity for (un-)foreseeable extended use (for example, by establishing databases or gathering health information).

While nearly exclusively focusing on the problem of gathering ever-more information about citizens and the possibility of 'identity theft' in its various manifestations, ranging from data to latent fingerprint theft, the public critical discourse in Germany, echoed by our interviewees, does not question at all common assumptions concerning the fingerprint. One is the uniqueness of one's fingerprint as a physical identity marker and hence its merit for criminalistics' purposes, a view that goes back to the beginnings of its application (Cole 2001). Another assumption concerns the ability to correctly identify and unambiguously decipher the fingerprint.¹⁸

There is little academic research that challenges this presumption by pointing out that fingerprint identification actually involves interpretation. It works on the basis of a 'mechanical objectivity' (Daston and Galison 2009: 121), erasing the 'human handprints from the scientific practice' (Magnet 2011: 11). The hermeneutical moment must be obliterated in support of the 'scientifity' of the presentation of 'natural facts' (Pugliese 2010: 38). Yet, both the reading and matching of fingerprint data are procedures that are better described by the notion of 'opinionisation'. Evidence, in other words, is a question of opinion rather than a fact; it is being established rather than merely measured (Cole 2008: 110, 2005). To be sure, the assumption of the uniqueness of one's fingerprint that defines the technology's merit is that it, at least currently, is impossible to falsify and implicitly serves as a precondition of individualisation; that is, of verifying and identifying individuals on the basis of their fingerprint.¹⁹ As a *pars pro toto*, it speaks

¹⁵ See Heribert Prantl (2012).

¹⁶ At least since 1978, German media discourses relate the idea of getting a glimpse into the inner and invisible world of the body or oneself to the surveillance practices imagined in George Orwell's dystopian world of *1984* (see 'Gläserner Mensch', *Der Spiegel* 17: 32-33, 13 February 1978).

¹⁷ George Orwell's *1984* itself evolved into a synonym for a dystopian world of governmental surveillance and a threat to privacy in the West (see Muller 2008: 214, especially for the UK media discourse, Barnard-Wills 2011). The degree to which the reference to Orwell has gained in currency is suggested by 'The Big Brother Award'. In Germany, this prize has been awarded annually since 2000 by the association 'digitalcourage' to various organizations, authorities, companies or individuals who have consistently threatened or violated people's privacy or impaired data protection. As a Big Brother Lifetime Award in 2005, it has been awarded to the Minister of the Interior, Otto Schily, among others for introducing the biometric passport.

¹⁸ It is probably for this reason that the case of the US lawyer Brandon Mayfield played little to no role in the German mass media, nor in our interviews. Since Mayfield's fingerprint allegedly had been found at the crime scene, he falsely came under suspicion and was ultimately arrested for having participated in the bomb attacks in Madrid in 2004.

¹⁹ For a history of individualisation protocols in Britain and the US, see Cole 2001.

the truth about one's identity—a truth that can hardly be challenged. By contrast, the deciphering methods are, for their part, barely verifiable. Criteria differ significantly among countries, for example, as to what should be taken as a basis of a matching procedure and what constitutes a match.²⁰ While promising substantial 'improvements over existing systems in the degree of distance, speed, accuracy and objectivity', new biometric identification technologies actually contributed to a 'long history' of standardising identification systems and stabilising identity that otherwise is 'a fundamentally unstable construct' (Gates 2006: 418).

The public discourse, by contrast, focuses for the most part on calling data security into question. The new electronic identity schemes are said to encourage criminal desire for 'hijacking entire identities' (Biermann 2010). Both the affirmative and the critical discourse, then, consider the isolation of identities on the basis of the data at hand be feasible. It is viewed, however, in terms of a diffuse threat that citizens need to be protected from, whether through biometric technologies, as the affirmative discourse has it, or by opposing them.

This concern was illustrated in 2008 in a spectacular campaign by the Chaos Computer Club (CCC). Here, the core argument of the affirmative discourse in favour of the introduction of biometric data devices in general and the digital fingerprint in particular—namely to prevent 'identity theft' and make the identity documents using a person's most individual markers safe—was turned on its head. Making an ironic statement, the Club presented to the public a copy of the digital fingerprint of the then Minister of the Interior, Wolfgang Schäuble, who had always argued in favour of the technology. The copy had been developed on the basis of a fingerprint that the minister had left on a glass. The hackers did not limit their campaign to only making the data public. Protesting against the political claim that the digital fingerprint was safe and employable for security purposes, they also included in each copy of their journal a dummy of the minister's fingerprint with an invitation to the reader to place the thin leaf onto her own fingertip so as to encourage its misuse (CCC 2008: 56-57).²¹ Again, what was called into question here was not the evidence of data being able to prove an identity, but rather its misuse on precisely this basis.

3. The interviews: narratives and imaginations

In scrutinising the conditions of acceptance, the research project's aim was indeed not to contribute to the usual mainstream discussion on how to enhance acceptance of a control and security technology, but rather to deconstruct that conception. We proceeded from the assumption that acceptance is something instable and depends not on invariable attitudes but on the context of the application of the technology, which includes the technical setting, the enrolment procedure as well as the forms of encounter with people and, most crucially, the officials involved. We also assumed that it makes a significant difference whether the digital fingerprint is applied in a private, commercial or public context. One of the most interesting settings turned out to be a registration office in Germany's second largest city, Hamburg, where the residents have to apply for, among other things, a new passport and ID. Since the ID with the digital fingerprint was supposed to be introduced as an optional choice in 2010, we sought to examine the conditions surrounding that choice. Our observations focused on how the technology and the option to have it integrated into the ID were officially promoted and presented to the residents in their face-to-face

²⁰ Whereas in Great Britain a minimum of 8 minutiae is necessary to establish identification (until 2005 it was a minimum of 16 minutiae), Italy's and France's standard is 16 points and Brazil and Argentina even require 30 matching ridge points (Meintjes-Van der Walt 2006: 166). Furthermore, in contrast to countries that subscribed to the 'Method for Fingerprint Identification' (Interpol European Expert Group on Fingerprint Identification), for those using the 'ACE-V' methodology (USA, Canada, Australia, New Zealand), creases or scars are additionally allowed as markers for individualisation (Langenburg 2012: 14-21).

²¹ The idea was not new: instructions on how to fashion fingerprint dummies of prints left unnoticed on everyday objects had already been published in 2005 (see Chaos Computer Club 2005: 14-16).

encounters with the authorities, and the response of the applicants of identity documents. The interviews we conducted afterwards inquired about both the digital finger-printing procedure itself and the digital fingerprint as a control and security device in general.

As mentioned above, the assessments of our interviewees echoed the public discourse in such a way that they drew on discursive figures of both the affirmative and the critical discourse—indeed independently of their acceptance or critical rejection of the digital fingerprint as an identification device. At the same time, none of the interviewees called the uniqueness of his or her fingerprint into question, as the following exemplary passage shows:

W: [...] everyone has his own fingerprint, and it really tells its own story, doesn't it? One that I don't think can actually be changed or altered.

A further interviewee contended:

C: Well, I look at it this way, eye colour and height, they're really external traits that tend only to be recognisable with the naked eye, and biometric data—biometric data make it possible to identify a human being with a hundred per cent certainty. [...] And that's the real difference. Each person has their own fingerprint.

Furthermore, none of the subjects interviewed questioned the validity of the fingerprint identification evidence with regard to, for instance, the traces people leave behind on the objects they touch or the so-called 'data double' (Haggerty and Ericson 2000). This is the reference fingerprint in databases, the template, for example, on RFID chips, or the artificial reproductions of the fingertip like those produced by the Chaos Computer Club. On the contrary, our interviewees saw an advantage in the fact that the biometric ID, which is supposedly non-forgable and non-replicable, provides more safety and is thus particularly useful for law enforcement purposes in the context of fighting terrorism:

K: Yeah, when I'm travelling I'm strangely very generous with my fingerprint, because I think that if one day everyone has given their fingerprint, it can be used precisely for the purpose of hindering the entry [...] of terrorists. That's why I actually don't think twice about it.

Apart from presenting vague threat scenarios from the affirmative discourse, such as terrorists entering the country, this passage is again testimony of a prevalent idea that none of our interviewees thought to question: that fingerprint technology is capable of clearly distinguishing one person from another, irrespective of time and place.

Ironically, it is against the background of this overwhelming confidence in the reliability of fingerprinting and the view of its inevitability as universal technology that a host of concerns has emerged. One worry is that the fingerprint leaves a clue that is directly traceable back to the owner:

C: No, with a fingerprint it's not actually a question of precise identification, but it has to do with the fact that the fingerprint has become famous for precisely the fact that everything that you touch can in effect be traced back to you. [...] A fingerprint is not only for identification. Everything that one touches can also be connected to you. And that's the thing. It's as if one makes available, or surrenders, all kinds of secrets just because one went to buy ice cream or something like that.

It is precisely this belief in the possibility of a clear identification, together with the understanding that we are not in control of all the traces we unwittingly leave behind, which incites feelings of insecurity. And, it is in this context that the figure of the 'transparent citizen', indirectly alluded to in the passage above, re-

emerges. The concern is that the fingerprint might contain, or conflate, all of a person's private data and secrets. The literal English translation from the German is the 'vitreous citizen', which further connotes fragility and translucence. In referring to this notion of the vitreous or transparent 'individual' (rather than citizen), however, the interviewees were fully aware of the metaphor's common understanding. Similar to the original model of the 'transparent homunculus', which shows the inner life of the body,²² the concern is that one becomes entirely accessible to the vigilant gaze of the state. As one interviewee explained:

Z: You are not actually transparent, you are visible. But you are to the extent that you make a payment somewhere and your debit card or your name shows up somewhere or... I call it a data set [...] Just what happens to the data set the moment you give up your information is not something you can know.

This quote articulates a further unease about the uncontrollable paths fingerprint data might take once they have been surrendered. Obviously, this fear grows the more personal data is processed, rendering the ostensibly suspicious visible. The data processing itself, however, remains rather opaque (see Merry 2011: 84; Marx 2002). The transparent self thus in a way contrasts with the non-transparent world of data storage and collation. Another interviewee couched his anxiety about his private data being collected by governmental authorities in literally a peculiar notion: becoming transparent, one might be 'nailed down' on the information the data contains.

Furthermore, the interviewees addressed what the critical literature on automated control technologies calls 'the reversal of the legal notion of innocence until proven guilty':

W: [...] they could have the fingerprint of somebody who has absolutely nothing to do with it, but from somewhere. And what happens then? The person's linked to a crime, even though it can be clearly proven that he wasn't at the scene. But that's just how it is... Isn't it?

While for one interviewee, refusing to provide a fingerprint in identity documents is already an indication of guilt, another rather describes his unease:

H: You're going across the street or doing some silly errands and then, all of a sudden, you're stuck in totally crazy situation. Someone tells you, 'You left your fingerprints there', all because I was at a mailbox two days earlier or something like that. It's nuts. But it's not a good feeling in any case.

In this case, the fingerprint, as if it were an artefact, takes on a life of its own. It becomes autonomous, separated from the body and independent of one's own will. And it is here that one and one are effectively put together for the sake of providing evidence. As stated in the initial interviewee quotation: once the digital fingerprint is part of the passport and data accessible to the police, in the case of some criminal act, they are 'able to prove that it's me' after I 'grab a cup of coffee'.

To sum up, then, there is a belief in the objectivity of fingerprinting that may be split into three features: a belief, first, in the uniqueness of the fingerprint; second, in the autonomy of the data, which is transmittable to any place (either virtually or physically) and; finally, in the evidentiary strength of the data, which may be unequivocally deciphered. The confidence in the objectivity of the fingerprint contrasts with and is at the same time the basis of a feeling of insecurity as regards the control over the

²² Originally, the 'transparent homunculus' was a 3-D anatomical human model made of a transparent shell by Franz Tschackert and exhibited in 1930 in the German Hygiene Museum in Dresden.

data. Both this unwavering confidence and feeling of insecurity are evoked and illustrated by our interviewees' preference for drawing on the fictive imageries of 'whodunits':

B: But the fingerprint—it's everywhere. If you watch something on TV, it's always the fingerprint. [...] Just like when you see a crime series, or whatever. The finger—the fingerprint—always comes first. That's the best evidence—which is just as you would expect, right?

In the following passage, the interviewee appears to conflate George Orwell and Orson Welles, thus calling to mind the eerie atmosphere usually associated with the latter's movies along with the idea of big-brother surveillance:

H: Orson Welles, the transparent person—how long has he been around? In how many places have I've been registered? [...] I'm probably registered everywhere.

At the same time, it became evident that the fictive world had a great deal of significance for our interviewees:

O: [...] I think it was James Bond, where... something was pulled over the fingertips and made a copy of someone's fingerprint. I don't know whether something like that is technically possible. In any case, the author [...] thought something up, like Jules Verne, that he thought was within the realm of possibility.

The allusion to Jules Verne here clearly affirms that although, or precisely because, his writing is science fiction, it may have anticipated at an earlier stage something that would come true sooner or later. Furthermore, the fictional character of James Bond stands for a real person and hence serves as a proof that the eventualities of identity theft and identity falsification are very real. Whereas science fiction is prediction or prevision,²³ 'real fiction' in this context concerns a possibility that merely has not yet materialised (Esposito 1998: 270). And as the campaign of the Chaos Computer Club indeed reminds us, the interviewee is not wrong to entertain 'real fictions'. Returning to the second interviewee quotation cited at the head of this article, we may also easily imagine that our fingerprint on a cup could be related to an 'al-Qaida guy', whose cup may also have been Osama bin Laden's, the figure representing the terrorist network in the affirmative discourse.

4. On objectivity and interpretation, imagination and truth effects

Critical security and Surveillance Studies take as their point of departure that our world is indissoluble from processes of interpretation and attributions of meaning. This means not only that what we perceive and how we act and think depends on the concepts and theories we maintain about the world. In particular, it also leads to a critique of our belief in the objectivity of automated control technologies and, in turn, their objectifying effects. Whereas the communication of today's automated control technologies, which are based on a binary code, seems to be unambiguous, Surveillance Studies stress that automatically generated data are not—and cannot be—detached from interpretation. The automated decision, for example, on what counts as a suspicious indicator of aberration in order to deny access, is inscribed into the technology (Pugliese 2010).²⁴ It is, in fact, the result of decisions made by human beings (Merry 2011). By the same token, the data produced by automated control technologies are interpreted once they are made into basic resource for a subsequent police or security measure. What is more, it is precisely

²³ As Nicolas Pethes (2004) observes, Orwell frequently is referred to as a prophet rather than a novelist.

²⁴ Pugliese's (2010: 30) argument goes much further in elaborating the colonial bias of the genealogy of biometrics where the 'white body' serves as the 'template'.

because these machines speak a binary language—not only in the sense of an algorithm but also in terms of either denying or permitting access—that their messages are largely non-negotiable, whereas their effect is one of dangerisation (Lianos and Douglas 2000); that is, of extending what may be attributed as dangerous or suspicious, aberrant or disruptive. Interpreting and negotiating the intention of a given individual and her personal motives in a social interaction is no longer relevant in automated control settings (Salter 2007), but rather binary distinctions ranging from black or white, male or female, to whether one has the adequate ticket or code available or not in order to either be accepted or rejected (Aas 2004; Goold and Lazarus 2007). It is against this backdrop that the reversal of the liberal legal ethos of innocence being presumed until guilt is proven and also the new pre-emptory forms of creating suspicion have been criticised. Automated control technologies not only screen data according to predefined norms, but also constitute norms of deviance and dangerousness within these procedures by algorithmically generating combinations of data and related expectations (Amoore 2007).

There are, then, different modes of producing and communicating norms within our social world involving meaning and narratives, on the one hand, and the binary logic of data coding, on the other. Biometrics here adds a further aspect. Corporeal features, as an object of control, are transformed into data and, in turn, become themselves suppliers of information. This kind of 'language' abstracts not only from a 'personal truth' as it is constituted in social interaction (Aas 2006: 153), but also from the bodies' 'words made of flesh' (Mordini 2009: 300). The 'purified' body is read as a document (Muller 2008). Rather than merely reducing corporeally embedded significations to a binary mode of thinking, the problem is again one of creating a new world of meanings, spaces of intervention and, indeed, facts: the body 'emerges as a source of instant "truth"' about the person to be granted or denied access and to be subjected to further security measures (Aas 2006: 154; Pugliese 2010).

If automated control technologies and, as the Italian sociologist Elena Esposito (1998: 290-2) observes, the new media in general produce 'instant truths' that emerge depending on the context in question, then we may well reconsider modernity's rather static conception of knowledge and truth. Rather than being about knowledge that is simply stored somewhere and ready for retrieval in order to tell the truth, our virtual world of automated control technologies is about information that is constantly been produced and reproduced. What counts as adequate or inadequate information depends on how we pose the question. It depends on the context and is largely procedural. Consider Google: any request produces its own response. There is no longer a single correct answer to a question—because there is no such single truth. This does not mean that the responses are arbitrary and that there is no verifiable truth. On the contrary, the response is contingent and truth literally a question of perspective: it turns out to be the effect of multilayered processes involving different forms of codification, technical arrangements and interpretations.²⁵

Furthermore, the notion of an 'instant truth' is illuminating with regard to the claim we have made in this article, again, in contrast to modern thinking that clearly distinguishes between a 'real reality' and a fictional world of imagination. The real and the fictive, facts and imaginations are not to be conceived of as two different worlds or realms of reality. Rather, they intermingle indistinguishably: the fictive figure of James Bond, for example, is real for our interviewees in that his actions in the movie render their versions of everyday life and, in particular, the rather opaque mechanisms of automated control technologies imaginable and comprehensible. In contrast to social phenomenology's conception of 'a single reality' encompassing the 'multiple' sites of our perceptual and behavioural activities within our everyday life world, what is at issue here then is rather a 'surplus of realities' (Esposito 2007: 68). Hence, our interviewees get the point precisely when evoking fictive imageries of total surveillance or social narratives of 'identity theft', thereby transgressing and countering the claims of the affirmative discourse

²⁵ On the notion of truth effects, see Foucault (2000); on the relevance of code and modes of codification with regard to the production of theory, see Galloway and Thacker (2007).

that maintains, for example, that biometric data as part of an ID would merely serve purposes of convenience or simply be more secure.

What is more, this also means that thinking critically about biometric technology while at the same time welcoming it as a reliable instrument of law enforcement, or even deciding in favour of voluntarily submitting a fingerprint as part of an ID, does not imply acting or thinking irrationally and inconsistently. Moreover, critical assessment does not involve rejecting the technology overall. Instead, it often accompanies the user's assertion of the technology's benefits, as shown in the case of one of our interviewees. The 45 year old man voluntarily accepts having his fingerprint in his ID, and when asked about his motivation, he responds that it would be 'the most secure' way to verify he is the legitimate owner of the document. This particular interviewee can be described as someone who is deeply convinced of the fingerprint's objectivity and yet still puts its preservation and, by extension, the security of his identity into doubt. Like several of our interviewees, he considers it impossible to completely avert data security breaches, data exchange and matching, which may have been previously denied as a political option, but tomorrow could become a normal fact of life. Media coverage offers several examples and narratives of 'identity theft' in the sense of replicating personal data and employing them in criminal acts. Today, this is even easier to accomplish with the digital fingerprint, since it is just a 'dataset'. In fact, the fingerprint technology tells us about exact profiles of individuals' whereabouts or habits that have been established digitally, as well as health data, revealing supposed 'hidden information' that had been secret. The interviewee described above is, indeed, right: 'one is visible' in the sense of personal data potentially being accessible at any time to unknown persons or even the vigilant gaze of governmental authorities. There may be no omniscient sovereign, but also no sovereign who protects our data. On the contrary, today's purported 'security situation' may warrant data exchange and collation. Our interviewee's assumption that his fingerprint will be stored at the local resident's registration office and matched by local police offices may be wrong in the present context, but also right in the sense that it is imaginable and, indeed, possible.

We thus learned from our interviewees that social acceptance is not only contextual, depending on the particular setting, interaction and procedure of application, but also essentially heterogeneous. There is no simple logic, for instance, of dystopian visions of control that determine a person's decision on whether or not to submit her fingerprint to a public authority. Moreover, it is not a question of whether narratives and fictions on data surveillance and the control options of digital fingerprinting are right or wrong. They simply do not follow such a dichotomy. Instead, they render the impermeable world of automated control technologies imaginable and thus accessible (similarly, see Magnet 2011: 6). As literary critic Jacinta Maria Matos (2012: 5) reminds us: 'Narrative is one of the most powerful cognitive instruments in our understanding of this world'. And fictions are experiments of thought and experiences 'in truth' (Simpson 2012: 104).

Certainly, in the field of governing security, the construction of 'emergencies' and security needs through social imageries has frequently been criticised (Calhoun 2004). It is 'affect politics' in that the imagined threat may become real since, as a fear, it is '*felt* to be real' (Massumi 2010: 53). Our anticipation of threats possibly materialising in the future literally renders them present, and the 'felt reality' subsequently legitimises pre-emptive action (ibid.: 54). It is in fact on the basis of the 'precautionary principle' (Ewald 2002) that scenarios demonstrating the advantages and disadvantages of biometrics are constructed. In other words, the fictive is employed as an invitation to others to imagine the 'what if' something undesirable happened in the future, be the vision one of ubiquitous identity theft or an encroaching dystopia like the one described in *1984*. We are prompted to be alert and worried by anticipating the 'worst possible'. The truth effects of such requirements are probably revealed most impressively by Donald Rumsfeld's infamous notion of the 'unknown unknowns'. Although contending that we are unable

to recognise and foresee the threats lurking, the very positing of this phrase makes the unknown real. In other words, a threat, however abstract, must be feared.²⁶

Thus anticipation, or the anticipation of threats, is not in itself right or wrong—the critical discourse does precisely this in order to deconstruct political promises on the safety of security technologies and security needs. The empirical question, rather, is what kind of imageries become prevalent within the discourse (Bright 2011). And, if the construction of these is a powerful tool of critique, this also implies that their deconstruction may be equally useful. The objectivity of the digital fingerprint, allegedly unambiguously decipherable and thus an ideal instrument of proof, is not only a fiction. It is also, as our interviews brought to light, a myth in Roland Barthes' (1972) sense, for as a signifier in fictional narratives it takes on a life of its own. As Simon Cole (2006) further shows, by analysing the logic of the repeated claims made by US-American fingerprint examiners to fend off the necessity of validating the individualisation process, this fiction of its objectivity is self-perpetuating. At the same time, it allows for the affirmation of the fingerprint as a useful tool of law enforcement and security purposes and the fear of its detecting powers and a critical stance on its serving as a tool of unrestricted surveillance. If the myth of the objectivity of the fingerprint is able to incite fantastic ideas and serves as a ground for justifying its technological improvement and further employment, as if there were no safety problems, we may turn this 'as if' on its head and challenge the present order precisely in the mode it presents itself to us: What if our world was much more ambiguous and unpredictable? What if we were able to counter the promises of the security technologies, seeing and foreseeing the manifold prospects of their being employed as surveillance technologies, without ourselves being simply and chronically suspicious?²⁷

The fictive, then, is not opposed to the real, and rather than representing a fictional reality, as Esposito (1998: 287) describes, it is a presentation of 'the reality of fiction'. It is, in the sense of Deleuze, a 'virtual reality' providing us with alternative 'constructions of possibilities'. Hence, imagining unknown futures, on the one hand, is a form of anticipation in the sense of conjecture: it includes a moment of inventing a reality yet to come (Aradau and van Munster 2007). On the other hand, it is a form of anticipation in the sense of foreseeing, which, at the same time, is a way of seeing: we can see a possible reality yet to come (Amoore 2007). And this exactly is 'the power' of the fictive: it is real in that we render the imaginary real and are able to articulate our critique.

References

- Aas, K.F. 2006. 'The body does not lie': Identity, risk and trust in technoculture. *Crime Media Culture* 2(2): 143-158.
- Aas, K.F. 2004. From narrative to database. *Punishment & Society* 6(4): 379-393.
- Amoore, L. 2007. Vigilant Visualities: The Watchful Politics in the War on Terror. *Security Dialogue* (Special Issue on Securitization, Militarization and Visual Culture in the Worlds of Post-9/11) 38(2): 215-232.
- Aradau, C. and R. van Munster. 2007. Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Future. *European Journal of International Relations* 13 (1): 89-115.
- Barnard-Wills, D. 2011. UK News Media Discourses of Surveillance. *The Sociological Quarterly* 52 (4): 548-567.
- Barthes, R. 1972. *Mythologies*. New York: Hill and Wang.
- Biermann, K. 2010. Ausländer brauchen den elektronischen Ausweis. *Die Zeit* online. 20 October 2010. Available at: <http://www.zeit.de/digital/datenschutz/2010-10/ausweis-auslaender-fingerabdruck/komplettansicht> (accessed 10 February 2013).
- Bitkom. 2008. (Federal Association for Information Technology, Telecommunications and New Media) *Mehr Komfort bei Grenzkontrollen an Flughäfen. (More convenience at border controls at airports)*. ePub. Available at: http://www.bitkom.org/files/documents/PI_BITKOM_und_ADV_Flughäfen_und_Biometrie_26_06_2008.pdf
- Boeing, N. 2006. Überwachungswirtschaft: Die unheimliche Welt der Daten. *Der Spiegel* online, 14 May 2006. ePub. Available at <http://www.spiegel.de/wirtschaft/ueberwachungswirtschaft-die-unheimliche-welt-der-daten-a-415706.html> (accessed 10 February 2013).

²⁶ 'Press Conference by US Secretary of Defence Donald Rumsfeld', NATO HQ, Brussels, 6 June 2002, available at www.nato.int/docu/speech/2002/s020606g.htm (accessed at 22 March 2013).

²⁷ On the option to act in a way that is contrary to politically and socially established modes of seeing and articulating, 'as if' these were not ineluctable frames, see Jacques Rancière (1998), drawing on Kant.

- Bourdieu, P. 1992. *Rede und Antwort*. Frankfurt/M.: Suhrkamp.
- Bright, J. 2011. Building Biometrics: Knowledge Construction in the Democratic Control of Surveillance Technology. *Surveillance & Society* 9(1/2): 233-247.
- Calhoun, C. 2004. A World of Emergencies. Fear, Intervention, and the Limits of Cosmopolitan Order. *Canadian Review of Sociology and Anthropology* 41(4): 373-395.
- Chaos Computer Club (CCC). 2005. Fingerabdrücke nachmachen leicht gemacht. *Die Datenschleuder* 84: 14-16. Epub. Available at: <http://chaosradio.ccc.de/media/ds/ds087.pdf>
- Chaos Computer Club (CCC). 2008. Basteltips Biometrieversand. *Die Datenschleuder* 92: 56-57. Epub. Available at: <http://ds.ccc.de/pdfs/ds092.pdf>.
- Cole, S.A. 2001. *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge: Harvard University Press.
- Cole, S.A. 2005. More than Zero: Accounting for Error in Latent Fingerprint Identification. *The Journal of Criminal Law and Criminology* 95(3): 985-1078.
- Cole, S.A. 2006. Is Fingerprint Identification Valid? Rhetorics of Reliability in Fingerprint Proponents' Discourse. *Law & Policy* 28(1): 109-135.
- Cole, S.A. 2008. The 'Opinionization' of Fingerprint Evidence. *BioSocieties* 3(1): 105-113.
- Daston, L. and P. Galison. 2009. *Objectivity*. New York: Zone Books.
- Esposito, E. 1998. Fiktion und Virtualität. In: *Medien – Computer – Realität*, edited by Sybille Krämer, 269-296. Frankfurt/M.: Suhrkamp.
- Esposito, E. 2007. *Die Fiktion der wahrscheinlichen Realität*. Frankfurt/M.: Suhrkamp.
- 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*. Brüssel. 24.11.2005. COM (2005) 597 final. Epub. Available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0597:FIN:EN:PDF>
- Ewald, F. 2002. The Return of Descartes's Malicious Demon: An Outline of a Philosophy of Precaution. In: *Embracing Risk*, edited by T. Baker and J. Simon, 273–302. Chicago, IL: Chicago University Press.
- Federal Commissioner for Data Protection and Freedom of Information. 2003. *Tätigkeitsbericht 2001 und 2002 des Bundesbeauftragten für den Datenschutz, 19. Tätigkeitsbericht* (19th Annual Report 2001 and 2002 of the Federal Commissioner for Data Protection and Freedom of Information.). Bundestag printed matter 15/888. 7 May 2003.
- Federal Ministry of the Interior. 2013. *Personalausweis*. Epub. Available at: http://www.bmi.bund.de/DE/Themen/Moderne-Verwaltung/Ausweise-Paesse/Personalausweis/personalausweis_node.html
- Federal Printing Office (Bundesdruckerei). 2013. *FAQs: elektronischer Reisepass (ePass)*. Epub. Available at: http://www.bundesdruckerei.de/sites/default/files/documents/2013/02/faq_epass.pdf
- Foucault, M. 2000. Truth and Power. In: *Power/Michel Foucault*, edited and transl. by J.D. Faubion, 111-133. New York: The New Press.
- Galloway, A.R. and E. Thacker. 2007. *The Exploit: A Theory of Networks*. Minneapolis: University of Minnesota Press.
- Gates, K. 2006. Identifying the 9/11 'Faces of Terror'. The promise and problem of facial recognition technology. *Cultural Studies* 20(4-5): 417-440.
- Goold, B. and L. Lazarus. 2007. Introduction. Security and Human Rights: The Search for a Language of Reconciliation. In: *Security and Human Rights*, edited by ibid., 1-24. Oxford, Portland/Oregon: Hart.
- Haggerty, K.D. and R.V. Ericson. 2000. The surveillant assemblage. *British Journal of Sociology* 51(4): 605-622.
- Iser, W. 1993. *The Fictive and the Imaginary: Charting Literary Anthropology*. Baltimore: Johns Hopkins University Press.
- Keller, R. 2005. Analysing Discourse. An Approach From the Sociology of Knowledge. *Forum Qualitative Social Research* 6(3), Art. 32. Available at: <http://www.qualitative-research.net/fqstexte/3-05/05-3-32-e.htm>
- Klein, I. 2011. Überwachte Sicherheit oder sichere Überwachung? Kulturelle Deutungsmuster im Diskurs um den biometrischen Reisepass. In: *Überwachungspraxen – Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle*, edited by N. Zurawski, 87–101. Opladen: Budrich UniPress.
- Langenburg, G. 2012. Scientific Research in the Forensic Discipline of Friction Ridge Individualization. In: *The Fingerprint Sourcebook*, edited by the U.S. Department of Justice/National Institute of Justice, chapter 14. Washington: CreateSpace Independent Publishing Platform.
- Lianos, M. and M. Douglas. 2000. Dangerization and the End of Deviance. *British Journal of Criminology* 40(2): 261-278.
- Magnet, S.A. 2011. *When Biometrics Fail. Gender, Race, and the Technology of Identity*. Durham and London: Duke University Press.
- Marx, G.T. 2002. What's new about the 'new surveillance'? Classifying for change and continuity. *Surveillance & Society* 1(1): 9-29.
- Massumi, B. 2010. The Future Birth of the Affective Fact: The Political Ontology of Threat. In: *The Affect Theory Reader*, edited by M. Gregg and G. J. Seigworth, 52-70. Durham, London: Duke University Press.
- Matos, J.M. 2012. George Orwell's Nineteen Eighty-Four: Is this where it all began? *Reconstruction: studies in contemporary culture* 12(3). Epub. Available at: http://reconstruction.eserver.org/123/Matos_Jacinto_Maria.shtml
- Meintjes-Van der Walt, L. 2006. Fingerprint evidence: probing myth and reality. *South African Journal of Criminal Justice* 19(2): 152-172.

- Merry, S.E. 2011. Measuring the World: Indicators, Human Rights, and Global Governance, with CA comment by John M. Conley. *Current Anthropology* 52(S3): 83-95.
- Mordini, E. 2009. Ethics and Policy of Biometrics. In: *Handbook of Remote Biometrics for Surveillance and Security*, edited by M. Tistarello, S.Z. Li and R. Chellappa, 293-309. Dordrecht, Heidelberg, London, New York: Springer.
- Muller, B.J. 2008. Securing the Political Imagination: Popular Culture, the Security Dispositif and the Biometric State. *Security & Dialogue* 39(2-3): 199-220.
- Petermann, T. and A. Sauter. 2002. *Biometrische Identifikationssysteme. Sachstandsbericht*, edited by Büro für Technikfolgenabschätzung beim Deutschen Bundestag. Arbeitsbericht Nr. 76. Epub. Available at: <http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab076.pdf>
- Pethes, N. 2004. EDV im Orwellstaat. Der Diskurs über Lauschangriff, Datenschutz und Rasterfahndung um 1984. In: *Medienkultur der 70er Jahre. Diskursgeschichte der Medien nach 1945*. Vol. 3, edited by Irmela Schneider, Christina Barz and Isabell Otto, 57-75. Wiesbaden: VS.
- Pugliese, J. 2010. *Biometrics. Bodies, Technologies, Biopolitics*. New York, London: Routledge.
- Prantl, H. 2012: Polizei soll Zugriff auf Fingerabdrücke erhalten. *Süddeutsche Zeitung*, 17 December 2012.
- Rancière, J. 1998. *Disagreement. Politics and Philosophy*. Minneapolis: University of Minnesota Press.
- Salter, M.B. 2007. Governmentalities of an Airport: Heterotopia and Confession. *International Political Sociology* 1(1): 49-66.
- Schily, O. 2004. Ausdauer, Disziplin und Einsatzbereitschaft fortführen – Rede vor dem Deutschen Bundestag am 11. Oktober 2001. In: *Nach dem 11. September 2001. Maßnahmen gegen den Terror. Dokumentation aus dem Bundesministerium des Innern*, edited by Bundesministerium des Innern, 30-36. Berlin.
- Simpson, Z. 2012. The Truths We Tell Ourselves: Foucault on *Parrhesia*. *Foucault Studies* 13 (May): 99-115.
- Taylor, C. 2002. Modern social imaginaries. *Public Culture* 14(1): 91-124.