10.6094/behemoth.2015.8.1.851

Gambling with the "Gift"?

On the Relationship between Security Technologies, Trust and Distrust. The Case of Fingerprinting

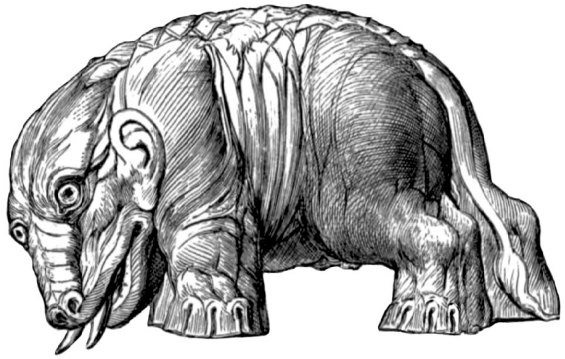
Sylvia Kühne

Abstract:

Trust is seen as a vital constituent of individual and cooperative action, being a value of its own. But the rise of automated control technologies in recent years, for instance digital fingerprinting, is described to be a development yielding distrust and inhibiting the establishment of trust-based relationships. This article critically pursues this thesis about the effects of new technologies of security and control for the "gift" of trust, by confronting the underlying general assumption with empirical data from a qualitative study on the social acceptance of fingerprinting in both governmental and commercial use. The article argues that, given the contextual circumstances in which the use of digital fingerprinting is embedded, on the one hand the use of fingerprinting does not necessarily lead to a culture of distrust and, on the other, that the relationship of trust, distrust and digital fingerprinting is more nuanced than depicted in the theoretical apprehensions.

Keywords: acceptance, biometrics, distrust, fingerprint, suspicion, trust

Sylvia Kühne is a research assistant at the Institute for Criminological Research at the University of Hamburg (Germany). She is currently writing her dissertation on the topic of digital fingerprinting, acceptance and trust. The work bases on the research project "Biometrics as 'Soft Surveillance'. On the acceptance of fingerprints" (funded by the German Research Foundation). **Email: sylvia.kuehne@wiso.uni-hamburg.de**



1. Introduction

In recent years the interrelationship of trust, distrust and new technologies has gained new momentum. The reason for this can be seen in the increasing deployment of a variety of information based technologies that have the capacity to record, store and collate personal details for purposes "of control, entitlement, management, influence or protection" (Lyon 2008, 2). The implementation of, in this sense, surveillance technologies raises concerns about the consequences of a growing reliance on especially more or less automated technologies. With reference to Georg Simmel (1950) or Anthony Giddens (1990), one could object that reliance on or trust in technologies for achieving certainty respectively trustworthiness under conditions of modern complexity has always been catalytic for surveillance systems (Nock 1993; Lyon 2001). However, the issue here is not only a change of objects or modes of trust. Given the increasing demand for technologies like digital biometrics, the role of symbolic tokens for establishing and maintaining trust is in question.

Initially introduced for security purposes by the state, digital fingerprint systems, among others, are also thus far "softly" (Marx 2006) becoming part of the citizen's daily lives, as they are nowadays marketed directly to individual consumers and commercial institutions. Given their prevalence as a technology to mark identities in national identity schemes as well as a payment device in supermarkets or schools, biometrics, like digital fingerprinting, serve as an emblematic example of extending "the realm of security" (Ceyhan 2008, 1). But basically they point towards how security is "constantly seeking to establish its markers of certainty and fixity" (1) by (technologically) interpreting all that is possible (Lodge 2013, 312). By scrutinizing the role of biometrics in realising "(in)security" and "quantum surveillance", Juliet Lodge (2013, 311f.) detects an "over-optimistic and unwarranted 'trust'" in their viability which, besides risky side effects caused by technological limitations, confront contemporary societies with various ethical, political and socio-legal implications.

Against this backdrop, scholars argue that instead of framing technologies like digital fingerprinting as technologies of security and control they are better conceptualized as "technologies of distrust" (Aas et al. 2008, 11), because they jeopardize people's ability to establish and maintain mutual trust (Aas 2006; Wood et al. 2006; Lyon 2009).

This article will discuss the relationship of trust, distrust and digital fingerprinting as an example of the new rise of automated control technologies. It aims to scrutinize the thesis that the increasing

implementation of security technologies contributes to a climate of distrust which underwrites a development where relying on technologies (of distrust) becomes a normal part of diverse relationship, thereby risking the 'gift' of trust.

In order to reveal the significance of the last paraphrase, the first section presents the outlined apprehensions of the consequences of biometric technologies on trust in detail, whereas in the second section this will be supplemented with sociological and philosophical conceptions of trust and distrust. Based on these theoretical grounds and drawing on a qualitative interview study on the social acceptance of digital fingerprinting **[1]**, in the following section I present some empirical insights on the role of trust and distrust in the context of using an automated control technology. In the final section I discuss these exemplary results **[2]** in comparison with the theoretical assumptions and demonstrate that a detailed analysis of contextual circumstances in which the use of digital fingerprinting are embedded provides a more nuanced picture of the interrelation of trust, distrust and automated technology.

2. Fingerprinting as a Technology of Suspicion, Putting at Risk the 'Gift' of Trust

Biometrics, especially fingerprinting, are evidentiary technologies or, as Joseph Pugliese put it, a "technology of capture" (2010, 2), which contribute to a 'long history' of standardizing identification systems (Gates 2006, 148; Cole 2001). Initially employed for administrative purposes, fingerprinting became a valued tool of criminalistics (Cole 2001). In Germany manual fingerprint analysis has been used by the police since 1903, which in 1993 became supplemented by an automated procedure using digitalized fingerprints for supporting legal prosecutions.

Although there have been attempts to establish digital fingerprinting as a pervasive technological device (for secure identity management as well as for convenience purposes), according to a study on behalf of the German Parliament until 2001 digital fingerprinting remained a niche technology beyond police applications (Petermann/Sauter 2002) **[3]**. But the situation changed with the political responses on the 9/11 terror attacks which not only laid the foundation for integrating digital fingerprints in national identity documents, but also for propelling the biometric industry's

[1] The main basis of the research on "Biometrics as 'Soft Surveillance'. On the acceptance of fingerprints" (funded by the German Research Foundation, 2010-2013) were observations followed by about 60 guided qualitative interviews. The contexts that have been studied comprised quite a diverse range of using fingerprint technology in different cities of Germany, these include: a video rental store where it has been installed as a device for access procedures, a supermarket and school canteens where fingerprinting serves as an alternative payment device, and a national registration office where citizens apply for national identity schemes. The focus on trust as a condition for acceptance evolved through the analysis of the interviews. Since it has not been a central concept of the study, it has rather been a surprising finding. In my PhD thesis I continue the analysis of the study by especially focusing on its meaning for accepting digital fingerprinting.

[2] Since it is my aim to present an insight in the relationship of trust, distrust and digital fingerprinting, rather than presenting the final results of the research, the article provides only exemplary findings.

[3] During the 1990s applications of digital fingerprinting could only be found in particular contexts, for instance for access control purposes in high security areas like nuclear power stations.

development in general. **[4]** Already on the 11th of October, in a speech to the German Bundestag, Otto Schily (2004, 35), then German Minister of the Interior, required that digital fingerprinting was to be used for identity documents as a protection from insecure identities. According to the Law on Combating International Terrorism **[5]**, amendments on the Passport Act (adopted 24 May 2007) as well as the Identity Card Act (adopted 18 June 2009) were adopted, allowing the integration of digitized biometric characteristics in German Passports and national identity schemes. Since 2007 digital fingerprints are mandatory elements of German passports, and in 2010 fingerprints became optional features of national ID cards.

The presentation of the fingerprint as a final security linkage between a person and her identity documents figured as one of the key features in the affirmative discourse. Daniel Meßner (2010, 16f.), among others, has pointed out that first and foremost the topos of "insecure identities" justified the political claims for a secure identity management and therefore facilitated the introduction of a technology which heretofore would have been criticized for being a tool for criminalization or "Volksdaktyloskopie" (general dactyloscopy). Hence, in the same speech Otto Schily (2004, 35) anticipated a general constraint for its general acceptance, an "emotional barrier" towards the use of fingerprints caused by its traditional criminalistics usage for determining suspects.

It is, in fact, against this backdrop that one line of critical argumentation arose. It refers for the most part to the critical discourse of civil rights organizations which from the beginning had a critical focus on the vast amount of control options coming along with the governmental use of, for example, digital fingerprinting. The line of reasoning mainly relates to the use of a technology which, to date and for the most part, has been used for law enforcement purposes but that now collects data of large parts of the population without cause and regardless of whether or not there is any actual suspicion (Gössner, 2002, 73; Kurz 2008, 104). It considers the introduction of fingerprints in identity papers to be a reversal of the principle of 'institutionalized distrust' which is apprehended to be a transformation of the relationship between governance and citizens (Prantl 2002, 9). The implementation of fingerprinting is read as a declaration of distrust and a general suspicion against the citizens, replacing trust in the citizens' autonomy by ascertaining and retaining information (Tauss 2008; Lyon 2007, 147), thus risking, as e. g. Benjamin Goold (2009) fears, to diminish institutionalized trust (Lodge 2013).

Withal there is a peculiarity with biometrics that leads to a second line of argumentation which

[4] For a brief overview on the German political economy of fingerprinting see Kühne/Wehrheim (2013).
[5] Gesetz zur Bekämpfung des internationalen Terrorismus ("Terrorismusbekämpfungsgesetz") dated 9 January 2002.

critically focuses on the increasing mediatization **[6]** of control (via physical representations) and thus interaction. In view of the fact that digital biometric technologies are used to yield certainty by 'translating' corporeal characteristics into mere information, again regardless of whether or not there is any actual suspicion, scholars from the field of Surveillance Studies are challenging the truth claim established by biometrics (Campbell 2004 **[7]**; Aas 2006, Cole 2008; Pugliese 2010). But they are not only identifying institutionalized distrust in the practice of control, but distrust is identified to be inherent to the logic and functional principle of digital biometric technologies themselves. With biometrics, bodies become "passwords" (Lyon 2001) that are fused into technology. If the latter hold an inscription for what counts as a suspicious indicator of aberration (Pugliese 2010), in automated control settings processes of verification and identification become automated decisions concerning a person's 'trustworthiness' and granting access or not. Social interaction, interpreting and negotiating the intention of a given individual and her personal motives, on the other hand, appear to be no longer relevant, because "when it comes to establishing the trustworthiness of strangers, an iris scan or a database of DNA samples and fingerprints, is quicker and is seen as more reliable than a story told in an interview" (Aas 2006, 144). Against this background, Katja Franko Aas (2006, 144) considers the contemporary rise of identification technologies based on biometric characteristics to be an indicator for a "profound social development [...,] a telling example of how they [society members] establish trust, or in this case, about the inability to establish trust through speech and linguistic communication."

To the extent that these technologies become self-evident in everyday life, they might contribute to a climate of doubt and distrust, as Nancy Campbell (2004) argues. In such a climate trustful relationships will not be taken for granted either between state and citizens or between parents and their children – the 'gift' of trust would be put at risk.

3. The 'Gift' of Trust – Conceptualizing Trust and Distrust

Grasping trust as an "incorporeal gift" (Rischmüller 2012, 300), first and foremost, refers to the great importance trust is generally attached to in the context of human sociality. Barbara Misztal, among others, emphasizes its importance as the 'prerequisite of order' (1996, 26ff.) because, following Goffman's account on normality, its "protective mechanism [...] prevents chaos and disorder by

[6] The term mediatization refers to the observation, according to which "social life becomes increasingly embedded within processes and systems of technological mediation." (Jansson 2012, 410)

[7] Surely, Campbell's argumentation (2004) refers to a different form of surveillance technology (drug testing), it nevertheless appears to be applicable to fingerprinting. Firstly, both technologies are forms of technologically meditated monitoring based on "natural facts" (Pugliese 2010, 38). And they are, secondly, based on a framework of trust in (scientific) expertise and reputation, within data are interpreted in ways that "conflate prediction with prescription." (79) Especially on the "opinionisation" of reading and matching fingerprints see for example Cole (2008) or Pugliese (2010).

providing us with feelings of safety, certainty, and familiarity" (2001, 312). In this respect, trust can be understood as a gift because it is seen as a vital constituent of individual and cooperative action as well as societal order by establishing and maintaining relationships (Garfinkel 1963; Giddens 1990; Barbalet 2006).

Its considerable significance as a resource for social interaction stems from the fact that it is generated by social interaction itself (Endreß 2012, 85; Garfinkel 1963). In his essay "Die Gabe" (Essay sur le don", "The gift") Marcel Mauss (1990) reasons that accepting a gift is accompanied with the obligation of reciprocity which can only be realized through trust, that is to say, by suspending the givers' uncertainty about the acceptor's future action. Accordingly, trust implicitly indicates a certain lack of information and knowledge. In other words, trust does not require evidence in terms of encompassing or explicit knowledge (Simmel 1950). On the contrary and in the words of Georg Simmel (1950, 318), trust is

> "a hypothesis regarding the future behaviour, a hypothesis certain enough to serve as a basis for practical conduct, [trust] is intermediate between knowledge and ignorance [...]."

If trusting someone means relying on somebody else's good will, as Annette Baier (1986, 234) has convincingly argued, the act of trusting implies becoming vulnerable to the limits of that good will. Provided that, trusting or taking the "leap of faith" (Möllering 2006) implies not only suspending uncertainty. Although trust, as a hypothesis, is precarious, that is to say "one leaves others an opportunity to harm one when one trusts", the act of trust "also shows one's confidence that they will not take it." (Baier 1986, 235) Put it another way, trusting also means suspending social vulnerability by acting "as if" the opportunities for harming the one who trusts were non-existent (Möllering 2006, 111; Baier 1986, 235).

Moreover, as trusting signifies that one deliberately refrains from encompassing knowledge as a means of control (Baier 1986; Luhmann 2000, 37; Hartmann 2011, 185f.), trust-based relationships can be understood to have a value in themselves. According to Annette Baier (1986) and Martin Hartmann (2011), the intrinsic value of trust can be attributed to the fact that trust, as a reliance on somebody else's good will without encompassing knowledge, means entrusting the trusted with "discretionary powers" (Baier 1986, 239). The pivotal essence of trusting therefore lies in

acknowledging another person's freedom of action to handle the things we value. This goes beyond an instrumental value of trust which enables the one who trusts to pursue her interests in cooperative ways. Accordingly and as Hartmann (2011, 185ff.) underlines, it is not possible to substitute trust by means of control without losing its intrinsic value.

In unraveling the metaphorical meaning of a "climate of trust", he states that the value of trust as a will to refrain from monitoring is, furthermore, normatively inspired (Hartmann 2007, 6). It bears upon "a collective reason [...] to act in a certain way that stems from the fact that others have this reason too" (5). The ability to trust as well as specific practices of trust are therefore highly related to what can be called a culture or climate of trust, because it points to the conditions under which acts of trust are possible (Hartmann 2007, 11; Gambetta 2001). Thus it seems reasonable to infer that cultures of trust enable for voluntary cooperative action, both on an individual level and concerning the relationship between citizens and government. Contrary to that, cultures of distrust might hamper the establishment of trustful relationships.

For Niklas Luhmann (2000, 93) distrust is driven by potent negative expectations or, as Patti Tamara Lenard (2008, 316) puts it, "reflects suspicion or cynicism about the actions of others". Such a conduct calls for defensive rather than collaborative action. Whereas trust is not grounded on evidence but on the absence of counter evidence (Gambetta 2001, 235; Hartmann 2007, 4), distrust, on the other hand, heavily relies on only a few but exaggerated signs or pieces of information. Following Luhmann's formulation, Lewicki et al. (1998, 446) see distrust as an expression of "wariness, skepticism, and such behavior as observed defensiveness, watchfulness, and vigilance" which can be observed in manifested social constraints as "monitoring mechanisms or bureaucratic and regulatory controls".

Certainly, from a sociological perspective, trust and distrust are neither good nor bad per se, as Martin Endreß (2012, 86; Lewicki et al. 1998) emphasizes. In a normatively neutral way distrust itself is as essential as trust and, as Luhmann posits (1979, 71), their relationship can be conceptualized as being "functionally equivalent". Piotr Sztompka (2000), for instance, considers distrust a key constituent in the trust-relationship between citizens and government and the "institutionalization of distrust" functions as a structural principle of democracy. 'Cultures of trust' and 'cultures of distrust' are therefore "bound in a dialectical relationship" (290), just as trust and distrust intermingle in a person's everyday encounters with reality (Endreß 2012, 88).

The problem with distrust, however, follows from an imbalance between trust and distrust. Luhmann (1979, 72) points to the problem according to which a person who distrusts is left "with little energy to explore and adapt to his environment in an objective and unprejudiced manner". Furthermore, by not trusting people and treating them as untrustworthy distrust tends to perpetuate itself (71ff.). The risk, therefore, lies in a 'culture of distrust' or conditions of "low trust/high distrust" (Lewicki et al. 1998, 446f.) in which actors are no longer voluntarily depending on each other because there is "no reason for confidence in another and ample reason for wariness and watchfulness" (ibd.). The reasons for distrust, however, might differ, as Lenard (2008, 317) argues: They can be based on knowledge that, for example, can be grounded on experiences of betrayed trust. But they can also spring from mere suspicion, which justifies cautious interaction. Whereas suspicious attitudes might lead to increased monitoring and control, such an engagement, again, as Deborah Welch Larson (2004, 35) argues, might also function as the "indirect indicators of distrust". Taking into account the growing significance automated control technologies have attained beyond state control, one might reason that suspicion disperses "not only within institutions, but beyond their real and virtual walls" (Campbell 2004, 79).

4. The Interviews: The Role of Trust and Distrust in Accepting Digital Fingerprinting

The lines of argumentation presented in the first part of the paper certainly address specific relationships of trust and distrust, and therefore varying forms of trust, from interpersonal trust to confidence and trust in governmental institutions to general trust. Nevertheless they, first and foremost, bear upon the controllers' perspectives and therefore pay critical attention to the purposes the technology might serve. But this also leads to the underlying assumption that there is an unambiguous meaning conveyed by automated control technologies. The qualitative study on the acceptance of fingerprinting, drawing on perspectives of sociological technology studies (Pinch/Bjiker 2012; Rammert 1999), precisely questioned this assumption. The project's aim was to scrutinize the conditions of acceptance, which was assumed to be something instable. Starting out from the assumption that acceptance cannot be deduced from technology itself and the user's invariable attitudes, it was

expected to be depending on the context of the application of the technology. Whereas this includes specific social and technical settings, enrolment procedures and ways of encountering people, the focus of the observations therefore was on how the technology was promoted and presented in their encounters with fingerprint takers and how applicants responded. Accordingly, the decision to use digital fingerprinting was expected to depend on the users' notion on the specific application and on how they appraise it. In qualitative interviews conducted afterwards, the interviewees therefore were inquired about both the digital fingerprinting procedure, digital fingerprinting in general as well as about the specific context of application.

Trust respectively distrust have not been central concepts since the very beginning of the study. Instead they evolved mostly through the examination of the users' assessments of fingerprinting. Its apprehended purposes are not only quite heterogeneous but the technology is also deemed to be quite ambivalent as a control and security technology in general, on the one hand, and the application in specific contexts on the other (see Krasmann/Kühne 2014). With regard to the interviewees there is a deep-seated belief that automated fingerprint systems function in an irrefutable and impartial manner. Assuming the uniqueness of their fingerprints, they are confident that fingerprint identification is a reliable technology capable of clearly distinguishing one person from another. As fingerprinting is therefore apprehended as an objective technology for representing individuals' identities – a perspective which is inherent to both the scientific and the security-policy discourse (Aas 2006, Cole 2006) – it is against this backdrop that the interviewees are expressing a feeling of unease. One of the main concerns is that each person or institution that gets access to the (digitally archived) fingerprint would be able to derive extensive profiles from it and also reveal all of a person's private data and secrets, for example their choice of borrowed DVD's or their buying habits. As a result, the interviewees express a certain degree of wariness and scepticism when it comes to the potential misuse of the technology for purposes of control and surveillance: it might affect the conduct of "civil inattention" (Goffman 1963 cit. in Endreß 2012, 88) and as a result their personal freedom. If such a misuse and uncontrollable surveillance is imaginable, this might result in a perception of ambiguous social conditions and unsettling trust in one's own expectations. But the further analysis **[8]** rendered that these risks as well as the meaning of fingerprinting as a suspicious technology of control are assessed differently, depending on the specific application context. Assessments base, on the one hand, on evaluations of trusting relationships, both in terms of a varying trustworthiness

[8] Based on the conceptions provided in the second section, the analysis proceeds from the assumption that trust isn't limited to a specific form or 'mode' (Endreß 2012), but ranges from reflexive balances of risk to conditions of preceding interactions (Möllering 2006; Hartmann 2011; Endreß 2012). Although the latter, for the most part, remain implicit or pre-reflexive, the formerly 'good reasons' as well as their reservations, nevertheless, can become reflexive and made evident in the analysis of qualitative interviews.

ascribed to different actors within the scope of dealing with the data, and the meaning of control and trust generally attributed to specific application areas. Given the specific relationship between those who control and those who are controlled, assessments, on the other hand, vary accordingly to the users' active involvement in utilizing a control technology.

4.1. Building on Trust

Drawing on the locutionary acts of trust found in the interviews, the analysis revealed that for many users trust plays an essential role for managing the ambivalence that using fingerprinting entails for them. For example, for customers of the supermarket and the DVD-story the reliability of their expectations that the use of fingerprinting will not be to their disadvantage is primarily established through a more or less direct face to face interaction with the respective provider. In reflecting on their motives of using fingerprinting, some interviewees, sometimes even surprising for themselves, referred to trust-based decisions and explicated their formerly 'good reasons' for trusting, as the following exemplary passage shows:

> Elisabeth Müller: And as I've said, since (*name of the supermarket/chain*) are here we've been buying there, and insofar, you know, there's a certain degree of basic trust at least from my side, to have it this way, you know? And also, this family has been local for a long time, they had a small shop, a bit further down the road, and also I was born here in (*name of the place/neighborhood*). It's also a question of, you know I wouldn't do this with any shop! **[9]**

What becomes clear from this quote is that in the context of the supermarket elements of familiarity are crucial. Based in a medium sized town, the supermarket, in a large part, attracts regular customers, like most of our interviewees. Here actual neighborhood is intertwined with propinquity which provides the users with a feeling of safety and certainty. The interviewee is referring to past experiences with the owner and how trust has implicitly provided the basis for ongoing interaction. Furthermore she emphasizes a shared history with the owner's family. Hereby she is expressing the idea of being part of a community where people at least met each other briefly which, for another interviewee, creates its own securing mechanism:

[9] Names of people and places from the research have been anonymized and quoted excerpts from interviews have been translated.

> Horst Bauman: [...] If something happens at (*name of the owner of the supermarket*), it won't go any further, will it?

Here the interviewee indicates an instrumental value that secures the limits of the owner's good will, according to which the owner's conduct would become well-known throughout the region. This can be read as the "rule of meeting again" ("Gesetz des Wiedersehens") Niklas Luhmann (2000, 46) regards as a characteristic of social contexts which already established stable relationships.

In contrast, customers of the DVD-store could not draw on long term experiences. This is due to the fact that submitting the fingerprint is a precondition of making use of the store. Therefore the users had to become familiar with the owner more or less instantly during the registration process. In the interviews reflections on the impressions the owner made for perceiving and evaluating his trustworthiness are central. "Impression management" can be, in James Henslin's (1968, 140) words, described as a condition for trust when "an actor has offered a definition of himself and the audience is willing to interact with the actor on the basis of that." The following passage from the interview with the owner of the DVD store exemplifies how he presented himself in personal encounters.

> Andre Beringer: And, I've always been telling the people that I've got a good reputation here, and they are welcome to ask about me, I've never handed out any address here, and these fingerprints, I've said to them, I couldn't hand them out because I don't know where they are.

This definition of himself of being sincere, which could be observed several times, has been experienced as valid and his argumentation as persuasive by most of the interviewees. The fact that in cases of technical problems the owner allowed users to contact him might have supported this assessment. As a result, from the users' perspective any misuse of data and potential data linking of fingerprint and movie data are considered to be highly unlikely because, as on interviewee argued, "somehow he conveyed that he's trustworthy" (Florian Berg). Trusting the owner therefore allows them to act as if these insecurities would not exist.

From the users' perspective, trusting the owner of the supermarket as well as that of the DVD store is justified because the company has a 'face' that relates to an identifiable person which, although not necessarily, is known personally. At least, even on bowing terms, knowing the owner (and his

family) serves as a prerequisite for participating in the fingerprint-procedure and leaving him with "discretionary powers" (Baier 1986, 239) of handling their fingerprints.

For applicants for national identity documents, familiarity with official procedures as well as interactions with public agency staff are essential elements of acceptance, but more in terms of routine and authority than closeness. In view of the fact that public policy and state action remain rather abstract, the interviewees' statements on trust are often normatively denoted, as shown by the following exemplary passage.

> Peter Jansen: Indeed, I do trust that they (the fingerprints) will be handled correctly. I must have trust in that. You know, if I couldn't have trust in that, … I wouldn't have any trust at all.

For Peter Jansen and a few other interviewees trust in the state is a value of its own. Phrases like these can be read as a "faceless commitment" (Giddens 1990), an expectation that in a democratic society those who are trustfully conferred options of control will not abuse their positions of power.

As the interviewees' ambivalence towards the technology results from the technology and the fact that the use of data tend to be inscrutable, trust (in persons or institutions) becomes important for, on the one hand, bridging this state of not knowing and, on the other hand, for assessing fingerprinting as a technology to which they are not subject of control.

4.2. Reservations on Trust

Despite several statements of willing to trust, as mentioned above, for some interviewees, most notably for those who submitted their fingerprints at the national registration office, trust in the state becomes irritated. The reasons for this do not refer to the technology as such but, again, to the contingencies its usage implies. A technology of control operating with digitalized data is perceived to be difficult to control, due to the fact that its functionality appears to be unpredictable and data security breaches, data exchange and the matching of data are considered impossible to completely avert. Having that in mind, for one interviewee the application of fingerprinting triggers trust reservations. While imagining security authorities matching data with his fingerprints, he concludes:

> Christian Zander: Well, if the worst comes to the worst, they certainly match data. If now, if now the judge must agree or not, … that's very doubtful, but if it's, let me have it this way, technologically possible, they do it. […] At one time or other they do it. […] That's, I'm sure about that.

By echoing the well-known criticism 'what is technically possible will be done', in this quote he articulates an unease about technological opportunities which puts the agency of institutionalized mechanism of control into question. The behavior of security authorities might become arbitrary and less accountable. From his point of view these are risks that establish a critical "threshold" (Luhmann 1979, 45, 73) for his trust in the state. His willingness to trust is therefore accompanied by suspicion concerning the current and future security ambitions of state authorities, apprehending that they will take more than granted to them and do not only care for that with which they are entrusted (Baier 1986).

Trust and the association of fingerprinting as a technology which might be used for various control purposes appear to be interdependent. On the one hand the users, by having trust in those taking their fingerprints, solve the uncertainty problem by denying any problems connected to uncertainties coming along with this technology, such as those taking the fingerprints actually having any control intentions. For others, perceiving fingerprinting as a technology which might be used for any control purposes by those taking the fingerprints proves to be a condition necessary for raising questions of trust at all. New control technologies which make use of digitalized data show the limits of benevolent behavior. Thus, also the intrinsic trust in specific circumstances, such as the relation of state and citizen, is then itself put into question. If institutionalized distrust serves for giving evidence to one's own trustworthiness (Sztompka 2000, 28), still its strength is based on mechanisms of self-control rather staying in the back (29).

That trust as a precondition for accepting the fingerprinting technology may just the same come along with, in other implementation contexts, interpreting fingerprinting as an expression of distrust becomes obvious by the following excerpt from an interview with a 19 years old student who was using fingerprinting in her school. With digital fingerprints in passports and identity schemes, in her perspective the state unfortunately reveals little commitment to trust. Although only theoretically speaking, she explained:

> Simone Berghof: Well, I don't really like that now. Well, yeah, simply because … I think it's a pity that trust in a-, yeah that the state doesn't really trust its citizens, you know, I don't know if the state thinks that everybody's a criminal or a terrorist or whatever.

This kind of perspective according to which the application of digital fingerprinting is an inappropriate declaration of suspicion, unreasonably assuming that each and every person is posing an imminent risk and thus declaring her untrustworthiness, is not limited to the context of state administration. Another interviewee, also theoretically, renders the application of fingerprinting for time and attendance recording problematic:

> Marius Tapfer: Somehow that's so … yeah so little trust, you know. Extremely little trust. […] as I said, I work at a laboratory where we are twenty staff members. […] that's a family thing, that will only work with trust. […] But then, this fingerprint, well I know for sure that the company doesn't trust me, otherwise they wouldn't control me.

The application of fingerprinting is not only criticized for being an indicator of generalized distrust – aiming at the whole person – based on mere suspicion rather than substantial grounds. Here the value of trust itself as a basis for social interaction is put into perspective. For Marius Tapfer the use of fingerprinting in a small working environment inhibits establishing and maintaining mutual trust in, more or less, institutionalized relationships where, however, a climate of trust is conceived to be pivotal.

The question of trust or distrust respectively when it comes to technologies of control then proves to be not only a question of the appropriateness of its use and the anticipated motivations of those controlling but also to be a question of which concrete or vague message is triggered by its use. If insofar there are indeed indications of how control technologies such as fingerprinting run the risk of forfeiting the 'gift' of trust, as a conclusion we will have a look at the point of view of those actually playing the role of controllers in the context of using the fingerprinting method.

4.3. Establishing Distrust

In enquiring the social acceptance of fingerprinting in schools we conducted interviews with parents at two schools who allowed or decided that their children use fingerprint payment in their school

canteens. Not different from the other fields of application, fingerprinting is perceived as a double-edged sword and trust as well plays an important role with managing the parents' ambivalence towards this technology. Nevertheless, for some parents the latter turns into an advantage as they utilize fingerprinting for their own, although pedagogical motivated, supervisory purposes. Digital fingerprinting at schools, as it has been advertised, serves as a technology that prevents children from losing or forgetting their lunch money. From parents' perspective, the technology also provides the capacity to make sure that their children eat regularly or eat the right food. This is facilitated by the fact that fingerprint payment is integrated in an online payment procedure and therefore allows for budget allocations and for the parents receiving detailed monthly accounts – conditions which provide specific benefits, as one father explains:

> Richard Flieger: I mean, for me the advantage is that one doesn't need larger amounts of cash and that parents may control their childrens' spending behavior. I give him (his son) five Euros, or ten, he may as well go to a discounter across the street and buy crisps and Coke. Which he'd love to do, and so it's also ring-fenced. But also I'm able to restrict his spending, by, well, after all he can spend only two Euros a day and cannot have five 'Milchschnitten' (choc bars) and bring his sandwich back home.

According to the common perceptions among interviewed parents, whereas the schools' surroundings are full of risky seductions, parents' intentions indicate creating of a risk free environment for their children. This is illustrated by the reference to "Milchschnitten", a popular product in Germany that is advertised as a light snack but has been widely criticized for its high ration of fat and sugar. But even though eating behavior is not called into question, parents question their children's ability to spend their money carefully. By making use of the system it becomes possible for them to extend their parental control to uncertain, not permanently visible action. This way they not only make sure that money will not be lost but *that* and, furthermore, *what* their children haven eaten. As far as they commence controlling their children's behavior from the distant, they stop relying on them to behave in a certain way and become quite intolerant of what until then has been ordinary child behavior. For parents, however, the use of the fingerprint system ensures 'responsible parenthood'. Caring for their health, for instance, creates a new necessity for distrusting their children. Furthermore, for Richard Flieger, the parent cited above, the use of the system becomes an implicit pedagogical vehicle for teaching his son responsible spending behavior:

> Richard Flieger: By way of the system I get detailed insight into what he (his son) has bought. [...] He knows I can, and if then and now there is an argue: What do you buy there, after all? Is that necessary? [...] You know, I wouldn't like to establish any control system, but this way I like, I think, I am able to show in black and white: O well, that's your spending behavior and you could change this and that, then you well get along better with your money.

Here reliance on and use of the system is extended from school to home. Based on the assumption that the fingerprint is unique, telling the truth about one's identity and therefore whereabouts, the data provided by the system are perceived to be beyond any discussion. This in fact leaves no scope of discretion and curtails interpersonal communication at home because the truth is unambiguously revealed on paper.

5. Conclusions

Trust-sensitive approaches pay critical attention to the intended and unintended effects of automated control technologies like fingerprinting. They take as their point of departure that current attempts to overcome uncertainty via means of control and information gathering begets new preemptory forms of creating suspicion, regardless of whether perceptions of increased insecurities lead to their application or the latter, in the sense of their way of functioning and the mere availability yielding new uncertainties. The concern is not merely that its governmental use, demonstrating that no one can be trusted, runs the risk of leading to a reversal of the liberal legal ethos of innocence and weakens the citizens' trust in governmental authorities. But the mere fact that in many mundane settings achieving trustworthiness becomes increasingly technologically mediated, using physical markers as "signifier(s) of intent" (Lodge 2013, 312) supersedes personalized trust.

The results from the analysis on the dynamics of trust and distrust in accepting fingerprinting as a new technology of security and control, however, indicate that it is very difficult to make general statements about the 'impact' of this technology on trust or distrust. The significance of the biometric technology hardly results from its capacity of authentication, nor is it generally grounded in a perception of increasing insecurity. Although users acknowledge the assumed motives of implementation, for example protection from terrorism or theft, advantages are first and foremost related

to specific purposes and its perceived utility. For users of fingerprinting, each application therefore possesses an 'embedded meaning' not only due to the technical **[10]** but also the social setting.

The analysis revealed that the meaning of an automated control technology can be superimposed by, more or less, personal interaction between actors who submit their fingerprint and those who provide the system and 'receive' the print. Perceived sincerity in personal encounters and visibility provide the grounds for trust. As also shown by the exemplary results, despite distrustful expectations (for instance towards how governmental agencies might deal with citizen's data), trust in the state as well as trust per se is highly valued. Here, trust instead of distrust serves as a prerequisite for using an automated technology which is generally associated with unforeseeable intentions of control.

Some users are able to deal with their ambivalence, whereas for others trust and distrust remain competing conducts and therefore conditions for their acceptance, as is the case even if an artificial line is drawn between those who actively control and those being controlled (in this case for demonstrating the implications of using digital fingerprinting in schools). Here the technology is perceived as beneficial and worrying at the same time. But pointing to parents' rationales, however, reveals that this distinction is quite relevant for questions of trust and distrust concerning automated control technologies, as indicated by the critical approaches presented in the first part of the paper. "Technologies of suspicion" constitute a social order which, as Nancy Campbell (2004) argues, rests upon distrust rather than trust. Their implementation might symbolize ever new insecurities in terms of adverse but avoidable outcomes of another person's action, which make it impossible to deliberately refrain from monitoring. Nevertheless, this does not necessarily mean that the attentiveness for these new uncertainties determines the decision for using the technology right from the start. Often at the beginning there is just a new and exciting technology, a tool that parents allowed their children to test. But once they are seizing the varieties of options provided by the technological system, they are gradually using these options of control. The analysis demonstrates that parents' reasons for less acknowledging their children's freedom of action are based on preventive intentions in which care and control are intermingling. Their usage therefore calls into question what has been unveiled as the intrinsic value of trust: the acknowledgment of somebody else's capacity to handle her freedom. Trusting someone can mean putting her in a position of giving evidence to her capacity to do something, but for the trusted ones this means acknowledging the given confidence and,

[10] In the DVD-store, for example, handling the technology follows quite naturally from the fully automated settings in the store. Here digital fingerprinting, as well as in supermarkets and school-canteens, is regarded as a more or less reasonable solution connoting access, rapid payment or protection from losing or forgetting cash or the user card. At the national registration office, on the other hand, the technology is not primarily perceived as a practical procedure but the fingerprint itself qualifies as a safety feature. Nevertheless, also here purposes of public authorities are superimposed by the importance identity papers have for the applicants. Therefore, filing the fingerprint serves to perfect the identity papers, which are personally important, and to add an unforgeable token to become fingerprintable in any case of emergency.

especially for a child developing a confidence as a trustworthy individual in a state of autonomy (Hartmann 2011). Conceivably, fingerprinting as a technology of parental control might constrain this autonomy. Here fingerprinting to some extent replaces communication because based on its functional principle it is perceived as being more reliable than personal statements.

The results show that trust and distrust are not simply opposite ends of a spectrum but coexisting mechanisms for dealing with uncertainty (Lewicki et al. 1998; Luhmann 1979/2000; Endreß 2012). Trust as well as distrust are not static, they are mutable and in that sense contextual as well as situational. For instance, questions of trust and distrust in regard to fingerprinting become crucial if the 'embedded applicability' is put into question. Questioning the motives for the technology's implementation can be intertwined with worrying about values of established relationships (between government and citizens or an employer and its employees) if the implementation of control technologies conveys a conduct of suspicion and, moreover, that the status and the dignity of individuals are not respected. In such cases digital fingerprinting is perceived as less being a risk for a general culture of trust but for specific institutionalized relationships. As Tom R. Tyler (1990) argues, the acceptance of governmental action bears upon the perception and experience of fair treatment. Citizens therefore do not comply with decisions of governmental institutions due to threat of sanctions but a belief that they act in favor of the citizens' interests and good. Fingerprinting can therefore be considered to strain these relationships, as perceived distrust could be countered with a more distrustful conduct instead of trusting and leaving oneself in a vulnerable position. Nevertheless, the ambivalence expressed by the interviewees may also be interpreted as a kind of healthy distrust towards e.g. the state's security ambitions.

The results, however, further indicate that, and Endreß (2012, 88) draws our attention to this, the interviewees do not simply trust or distrust, because reality is much less unambiguous. Often they find themselves struggling with varying assessments or incompatible and inconsistent beliefs. Trusting or distrusting fingerprinting as a form of control can be ambivalent and can refer to different aspects as (a specific meaning of) the technology or its (vague or opaque) purposes. Thus, some reservations regarding trust, which are met with many interviewees, does not at all indicate the establishment of a general culture of distrust, as suspected by the Surveillance Studies and the critical civil rights discourse.

References

Aas, K. F. (2006) The body does not Lie: Identity, risk and trust in technoculture. In: *Crime, Media, Culture*: *An International Journal* 2(2): 143-158.

Aas, K. F.; Gundhus, H. O.; Lomell H. M. (2008) Introduction: Technologies of (in)security: 1-18. In: Aas, K. F.; Gundhus, H. O.; Lomell H. M. (eds.): *Technologies of InSecurity: The Surveillance of Everyday Life*. Abingdon et al.: Routledge-Cavendish: 1-17.

Baier, A. (1986) Trust and Antitrust. In: *Ethics* 96(2): 231-260.

Barbalet, J. (2006) *A Characterization of Trust and its Consequences*. ESRC priority network 'Social Contexts and Responses to Risk' (SCARR). University of Kent at Canterbury. http://www.kent.ac.uk/scarr/publications/Barbalet%20Wk%20Paper%282%29%2013.pdf (14/03/2014).

Campell, N. D. (2004) Technologies of Suspicion: Coercion and Compassion in Post-disciplinary Surveillance Regime. In: *Surveillance and Society* 2(1): 78-92.

Ceyhan, A. (2008) Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics. In: *Surveillance and Society* 5(2): 102-123.

Cole, S. A. (2001) *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge: Harvard University Press.

Cole, S. A. (2006) Is Fingerprint Identification Valid? Rhetorics of Reliability in Finger-print Proponents' Discourse. In: *Law & Policy* 28(1): 109-135.

Cole, S. A. (2008) The 'Opinionization' of Fingerprint Evidence. In: *BioSocieties* 3(1): 105-113.

Endreß, M. (2012) Vertrauen und Misstrauen – Soziologische Überlegungen. In Schilcher, C.; Will-Zocholl, M.; Ziegler, M. (eds.) *Vertrauen und Kooperation in der Arbeitswelt*. Wiesbaden: VS Verlag für Sozialwissenschaften: 81-102.

Gates, K. (2006) Identifying the 9/11 ‚Faces of Terror'. The promise and problem of facial recognition technology. In: *Cultural Studies* 20 (4-5): 417-440.

Gambetta, D. (2001) Können wir dem Vertrauen vertrauen? In: Hartmann, M.; Offe, C. (eds.) *Vertrauen. Die Grundlage des sozialen Zusammenhalts*. Frankfurt/M.; New York: Campus: 204-237.

Garfinkel, H. (1963) A Conception of, and Experiments with, 'Trust' as a Condition for Stable Concerted Actions. In: Harvey, O.J. (ed.) *Motivation and Social Interaction*. New York: Ronald Press: 187-238.

Giddens, A. (1990) *The consequences of modernity*. Cambridge: Polity.

Goold, B. (2009) Technologies of surveillance and the erosion of institutional trust. In: Aas, K. F.; Oppen Gundhus, H.; Mork Lomell, H. (eds.): *Technologies of Insecurity: The Surveillance of Everyday Life*. New York: Routledge-Cavendish: 207-218.

Gössner, R. (2002) Kollateralschäden an der "Heimatfront". In: *Ossietzky. Zweiwochenschrift für Politik/Kultur/Wirtschaft* 2. http://www.sopos.org/aufsaetze/3c764f6821a7e/1.phtml (10/09/2013).

Hartmann, M. (2007) *What is a climate of trust?* Lausanne October 3-5, 2007. http://www.unige.ch/sciences-societe/socio/pdrs/programme/20072008/collectifsmorges/HartmannWhatisaclimateoftrust.pdf (14/05/2013).

Hartmann, M. (2011) *Die Praxis des Vertrauens*. Berlin: Suhrkamp Verlag.

Henslin, J. (1968) Trust and the Cab Driver. In: Truzzi, M. (ed.): *Sociology and Everyday Life*. Englewood Cliffs: Prentice-Hall: 138-157.

Jansson, A. (2012) Perceptions of surveillance: Reflexivity and trust in a mediatized world (the case of Sweden). In: *European Journal of Communications* 27(4): 410-427.

Krasmann, S.; Kühne, S. (2014) 'My fingerprint on Osama's cup.' On objectivity and the role of the fictive regarding the acceptance of a biometric technology. In: *Surveillance & Society* 12(1): 1-14. library.queensu.ca/ojs/index.php/surveillance-and-society/issue/view/Open_2014 (12/07/2014).

Kurz, C. (2008) Biometrie nicht nur an den Grenzen. Erkennungsdienstliche Behandlung für jedermann. In: Gaycken, S.; Kurz, C. (eds.): *1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien*. Bielefeld: Transcript Verlag: 101-116.

Kühne, S.; Wehrheim, J. (2013) Versicherheitlichung und Biometrie. Zur Verbreitung einer Kontrolltechnologie im Spannungsfeld von Staat, Ökonomie und Alltag. In: Klimke, D.; Legnaro, A. (eds.): *Politische Ökonomie und Sicherheit*. Weinheim; Basel: Beltz Juventa: 303-318.

Larson, D. W. (2004) Distrust: Prudent, If Not Always Wise. In: Hardin, R. (ed.) *Distrust*. New York: Russell Sage Foundation: 34-59.

Lenard, P. T. (2008) Trust Your Compatriots, but Count Your Change: The Roles of Trust, Mistrust and Distrust in Democracy. *Political Studies* 56: 312–332.

Lewicki, R. J.; McAllister, D. J.; Bies, R. J. (1998) Trust and Distrust: New Relationships and Realities. In: *The Academy of Management Review* 23(3): 438-458.

Lodge, J. (2013) Nameless and Faceless: The Role of Biometrics in Realizing Quantum (In)security and (Un)accountability. In: Campisi, P. (ed.) *Security and Privacy in Biometrics*. London: Springer: 311-337.

Luhmann, N. (1979) *Trust and Power*. New York: John Wiley, New York.

Luhmann, N. (2000) *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität*. Stuttgart: UTB.

Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*. Buckingham, Philadelphia: Open Univ. Press.

Lyon, D. (2007) *Surveillance Studies: an overview*. Cambridge et al.: Polity Press.

Lyon, D. (2008) *Surveillance Society*. Talk for Festival del Diritto, Piacenza, Italia: September 28 2008. http://www.festivaldeldiritto.it/2008/pdf/interventi/david_lyon.pdf (25/10/2013).

Lyon, D. (2009) *Identifying citizens: ID cards as surveillance*. Malden. Cambridge: Polity.

Marx, G. T. (2006) Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information – "Hey Buddy Can You Spare a DNA?" In: Monahan, T. (ed.): *Surveillance and Security. Technological Politics and Power in Everyday Life*. New York: Routledge: 37-56.

Mauss, M. (1990) *Die Gabe. Form und Funktion des Austauschs in archaischen Gesellschaften*. Frankfurt/M.: Suhrkamp.

Meßner, D. (2010) Volksdaktyloskopie: Das Fingerabdruckverfahren als Überwachungsphantasie zwischen Ausweitung und Widerstand. In*: Journal for Intelligence, Propaganda and Security Studies* 1: 7-19.

Misztal, B. A. (1996) *Trust in Modern Societies. The Search for the Bases of Social Order*. Cambridge: Polity Press.

Misztal, B. A. (2001) Normality and Trust in Goffman's Theory of Interaction Order. In: *Sociological Theory* 19(3): 312-324.

Möllering, G. (2006) *Trust: Reason, Routine, Reflexivity*. Oxford: Elsevier.

Nock, S. L. (1993) *The Costs of Privacy: Surveillance and Reputation in America*. New York: Walter de Gruyter.

Petermann, T.; Sauter, A. (2002) *Biometrische Identifikationssysteme – Sachstandsbericht. Büro für Technikfolgenabschätzung beim Deutschen Bundestag*. Arbeitsbericht Nr. 76. Berlin. http://www.tab-beim bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab076.pdf (12/06/2013).

Pinch, T. J.; Bijker, W. E. (2012): The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other, in: Pinch, T. J.; Bijker, W. E.; Hughes, T. P. (eds.): *The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology*. Cambridge; London: MIT-Press: 11-44.

Prantl, H. (2002) *Verdächtig. Der starke Staat und die Politik der inneren Unsicherheit*. Hamburg: Europa Verlag.

Pugliese, J. (2010). *Biometrics: Bodies, Technologies, Biopolitics*. New York, Oxon: Routledge.

Rammert, W. (1999) *Technik. Stichwort für eine Enzyklopädie*. Technical University Technology Studies: Working Papers, 1-1999, http://nbn-resolving.de/urn:nbn:de:0168-ssoar-8811 (20/04/2013).

Rischmüller, F. (2012) Gabe und Vertrauen. Eine französische Perspektive. In: Schnabel, A.; Schützeichel, R. (eds.): *Emotionen, Sozialstruktur und Moderne*. Wiesbaden: Springer VS: 299-315.

Schily, O. (2004) „Ausdauer, Disziplin und Einsatzbereitschaft fortführen" – Rede von Bundesminister Otto Schily vor dem Deutschen Bundestag am 11. Oktober 2001. In: Bundesministerium des Innern (ed.) *Nach dem 11. September 2001. Maßnahmen gegen den Terror. Dokumentation aus dem Bundesministerium des Innern*. Berlin: 30-36 http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2004/Nach_dem_11_September_2001_Massnahmen_Id_95066_de.pdf?__blob=publicationFile (10/03/2014).

Simmel, G.; Wolff, K. H. (ed.) (1950): *The Sociology of Georg Simmel*. Translated, edited and with an introduction by Kurt H. Wolff. New York; Toronto: The Free Press.

Sztompka, P. (2000) Does Democracy Need Trust, or Distrust, or Both? In: Jansen, S. A.; Schröter, E.; Stehr, N. (eds.) *Transparenz: multidisziplinäre Durchsichten durch Phänomene und Theorien des Undurchsichtigen*. Wiesbaden: VS Verlag für Sozialwissenschaften: 284-291.

Tauss, J. (2008) Vertrauen in der Informationsgesellschaft. In Klumpp, D.; Kubicek, H.; Roßnagel, A.; Schulz, W. (eds.) *Informationelles Vertrauen für die Informationsgesellschaft*. Berlin: Springer: 63-70.

Tyler, T.R. (1990) *Why People Obey the Law*. New Haven: Yale Univ. Press.

Wood, D. M. (ed.); Ball, K.; Lyon, D.; Norris, C.; Raab, C. (2006): *A Report on the Surveillance Society*. Wilmslow: Office of the Information Commissioner; Surveillance Studies Network. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application%20/surveillance_society_full_report_2006.pdf (14/03/2012).