DIIS REPORT

DIIS REPORT

BIOMETRICS AS SECURITY TECHNOLOGY

EXPANSION AMIDST FALLIBILITY

Katja Lindskov Jacobsen

DIIS REPORT 2012:07

DIIS · DANISH INSTITUTE FOR INTERNATIONAL STUDIES

Danish Institute for International Studies, DIIS
Strandgade 56, DK-1401 Copenhagen, Denmark
Ph: +45 32 69 87 87
Fax: +45 32 69 87 00
E-mail: diis@diis.dk
Web: www.diis.dk

Cover photo: Masterfile/Scanpix
Layout: Allan Lind Jørgensen
Printed in Denmark by Vesterkopi AS

ISBN 978-87-7605-503-5

Price: DKK 50.00 (VAT included)
DIIS publications can be downloaded
free of charge from www.diis.dk
Hardcopies can be ordered at www.diis.dk

This publication is part of DIIS's Defence and Security Studies project which is funded by a grant from the Danish Ministry of Defence.

Katja Lindskov Jacobsen, PhD, Project Researcher
klja@diis.dk

Indhold

Abstract

Biometric technology has been afforded a central role in the security architecture that Western governments have forged since the events of 9/11 2001. With biometrics the body becomes the anchor of identification. In a security architecture centred on identification of persons of interest and determination of their status as friend or foe, biometrics has come to be praised for its supposedly exceptional capacity to identify reliably.

This report situates the use of biometrics as a security technology in relation to this promise of superior identification on the one hand and, on the other, to the various concerns that critics have raised. It argues that it is vital that decision makers acknowledge how biometrics is neither a flawless nor a politically neutral technology. Unless caution and concerns are taken seriously the risk is that biometrics will produce new forms of insecurity – rather than increased security.

Dansk resumé

Biometrisk teknologi er blevet tilskrevet en afgørende rolle i den antiterror sikkerhedsarkitektur, som den vestlige verden har fabrikeret siden 11. september 2001. Nogle anser ligefrem biometrisk teknologi for at være uundværlig i en tid, hvor fjendebilledet i international politik har ændret sig i en sådan grad, at identifikation af potentielle fjender kræver nye metoder. I en sådan kontekst er den biometriske teknologis løfte om usædvanlig præcis identifikation (af potentielle terrorister) en attribut, der har givet teknologien en helt særlig status i kampen mod terror.

Siden biometri blev indført som antiterrorteknologi, har brugen af biometri imidlertid bredt sig. Nu anvendes biometri f.eks. også i kampen mod pirateri. På den ene side anses biometri således for at være en uundværlig sikkerhedsteknologi, hvis anvendelighed øjensynligt ikke begrænser sig til hverken antiterror eller antipirateri. På den anden side, og i kontrast til denne fremstilling, har eksperter påpeget, at biometrisk teknologi har nogle afgørende begrænsninger, som det kan være omkostningsfuldt at overse.

Nærværende rapport uddyber dette paradoks om den biometriske teknologis samtidige udbredelse og fejlbarlighed. Vigtigheden af en klarlægning af dette paradoks skal ses i lyset af, hvordan biometri i stigende grad anvendes i mangeartede opgaver – ikke blot militært, men i stigende grad også humanitært.

Rapporten argumenterer, at det er afgørende, at beslutningstagere ikke ser teknologien som et neutralt værktøj og ikke lader sig forføre af biometriens løfter om ufejlbarlig identifikation. Det anbefales derimod at beslutningstagere er være opmærksomme ikke alene på teknologiens tekniske begrænsninger, men også på de politiske effekter som brugen af biometrisk teknologi nødvendigvis har.

Introduction

Following the events of 11 September 2001, various biometric technologies – including face, fingerprint and iris recognition – were quickly endorsed as cure-all solutions by politicians confronted with what was called the 'new threat of global terrorism' (see, for example, Lyon 2008; Magnet 2011). Since then new biometric techniques – such as gait recognition, palm vein recognition (Williams 2005; Zhang et al. 2011) and thermograms – have been added to the repertoire and more are in the pipeline (Visiongain 2008). Amidst this development of new biometric technologies and their endorsement as solutions to variously defined threats to security, this report shows how an important paradox can be observed, which needs to be considered when contemplating the use of biometrics in contemporary policies aimed at realising a given conception of security. On the one hand, an increasing number of actors have voiced serious concerns about the fallibility of various biometric technologies. Yet, on the other hand, the deployment of biometrics as a security technology continues to expand and to mirror the definition of new threats in international security.

This report explores this paradox by outlining some key limitations (five technical and two contextual) to the promise of superior security through biometric technology. Expanding on this point the report then shows how, despite these limitations, biometrics used as a panacea for variously defined 'threats' continues to expand, with biometrics moving on from being used as an anti-terror technology to now being introduced in the fight against seaborne piracy. It will then be suggested that it is worrisome that these limitations are rarely taken seriously when decisions are taken to deploy biometrics to deliver superior security and, moreover, that making blind faith in biometrics the security solution in the face of various phenomena defined as threats to contemporary society entails considerable risks.

The aim of this report is not so much to define an unproblematic alternative to biometrics, but rather to demonstrate why a thorough awareness of the technology – its limitations and political implications – is necessary in order to ensure a responsible use of biometrics as a security technology, i.e. a deployment that takes into consideration the technology's limitations including the different ways in which biometrics might produce new forms of insecurity, and certainly will do so if promises to provide superior security are trusted blindly.

The promise of superior security through biometric technology

Considering the development of security policies, we can observe a shift towards an increasing concern with identity and an accompanying focus on the need for new identification technologies to ease and speed up the task of identification on the assumption that this will offer greater security (see, for example, Muller 2011; Latham 2010). This is arguably a trend that the introduction of ideas such as 'governmental identity management' bear witness to (Strauß 2011). In other words, security and defence are no longer just a question of observing whether a neighbouring state is increasing its weaponry or carrying out research into novel defence technology that is perceived as a threat. Today, an additional security concern is the problem of accurately identifying which individuals are regarded as embodying the potential to become a *future* threat – one that security policies need to target and act upon before this potential materialises as reality. Indeed, it has been noted that confronted with these new threat perceptions: "defence and intelligence communities require automated methods capable of rapidly determining an individual's true identity as well as any previously used identities and past activities" (U.S. National Science and Technology Council 2006). In this particular context, identification has thus come to be regarded as a prerequisite for countering contemporary threats before they materialise as reality, a prerequisite for security from individuals who are defined as portraying a potential to become 'threats'.

Similarly, it has been noted that: "as the scope of threats are [*sic*] widening with globalisation, the targets are becoming individuals" (Karacasulu 2006). It is within this context that biometric technology has gained prominence, given its claim to produce a specific type of knowledge needed for such types of identification: biometric technology is not only capable of linking a person to past activities and/or monitoring a person's present activity. More than that, the collection and storage of biometric data allows for 'data mining', i.e. a process that extracts predictions about a person's future 'becoming' from his or her biometric data and, in that way, promises to deliver superior knowledge about who might and might not come to be of particular danger (Hildebrandt and Gutwirth 2008).

Considering these developments, this report will critically explore this promise of superior security through the deployment of biometric technology. Various questions will be asked, such as: what is the nature of this biometric knowledge? Can biometrics be said to simply have identified 'dangerous' individuals or might these recognition processes and the practices surrounding them actually

have contributed to the production of 'dangers' that did not exist in that form previously?

Focusing on the use of biometrics as a security technology, this report examines the defence and intelligence community's reliance on biometrics as the solution to variously defined threats to contemporary security (U.S. National Science and Technology Council 2006: 6). Specifically the report identifies two different types of limitations (technological and contextual) and suggests that careful attention to these limitations is critical in order to achieve a responsible deployment of the technology – a point that is arguably of particular importance given the present tendency to expand the use of biometrics as a security technology to newly-defined threats such as seaborne piracy.

To obtain information about the technological aspects of biometrics as well as the political context within which the technology is deployed, the material that this report draws upon falls into three analytically distinct categories: technology reports, government-commissioned papers and social science articles. In part one of the report, documents will be analysed with a focus on a number of limitations to the promises and expectations that currently surround the deployment of biometrics as a security technology. In part two, the focus of the analysis shifts from an exploration of the technology in 'isolation', to an analysis of the context – more specifically, the different types of agency that must be considered when deploying biometrics to realise a political objective, e.g. a specific conception of security.

PART ONE: LIMITATIONS

> "Questions persist ... about the effectiveness of biometric systems as security or surveillance *mechanisms, their usability and manageability, appropriateness in widely varying contexts, social impacts, effects on privacy, and legal and policy implications."* (Pato and Millet 2010: 1)

Biometrics can be defined as "any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or verify the claimed identity of an individual", (Woodward et al. 2003: 1). An important point must be added to this simple definition of biometrics, namely that contemporary biometric technologies entail the digitalisation of the unique body part – a process that has implications for the knowledge produced from the processing of this digitalised biometric data and hence for the body subjected to this technology, in particular given the possible political use of such biometrically-derived knowledge. Although biometrics is readily endorsed by various governments and presumed to be a vital security technology when confronted with the novelty of variously defined contemporary threats and dangers, it is important to note the central limitations of the technology in the process of security management. In what follows I will elaborate on five such limitations as a way in which to illustrate why a thorough understanding of the technology is needed when deciding to deploy it as a solution through which to attain a certain conception of security.

Technological Limitations

Non-uniqueness

Biometric recognition is probabilistic – it is not an absolutely accurate and certain identification technology and, according to critics, this is one of the technology's key limitations. In other words, biometric systems will always only provide a probability of verification. In a recent report from the U.S. National Research Council this point is highlighted as the prime challenge to the promise of greater security through the use of biometric technology. As the authors of the report point out, biometric recognition is "inherently probabilistic, and hence inherently fallible" (2010: 1). This limitation has not gone unnoticed by technology developers and system designers. Indeed, there have been moves to manage the probabilistic nature of biometric matching and the challenges that this represents, for example by introducing 'multi-modal biometrics'

such that the uniqueness of a match (i.e. the likelihood of making a correct match) increases with the number of biometrics that are combined (i.e. whilst it is likely that someone might have a fingerprint pattern that matches yours, it is far less likely that someone will have both a fingerprint and an iris image which match yours). In other words: "the fusion of multiple biometrics helps to minimise the system error rates" (Mane and Jadhav 2009: 90).

However, the use of multi-modal biometric systems then entails a different set of limitations and challenges. First, multi-modal biometrics is more expensive as it requires more data to be collected and processed. Besides that, another challenge confronting the implementation of multi-modal biometric systems is that a crucial question still remains unresolved; namely the question of "what are the best combinations (modalities)?" (Kumar et al. 2010: 5). Moreover, multi-modal biometric systems are also challenging to implement because of the complexities involved in making decisions "about the processing architecture to be employed in designing the multi-modal biometric system as it depends upon the application and the choice of the source. Processing is generally complex in terms of memory and or computations." (Kumar et al. 2010: 5) Besides that, there are also still a number of unresolved issues about the scalability of multi-modal biometric systems (Mane and Jadhav 2009). Finally, increasing the amount of biometrics being collected from an individual might increase the performance of the system but might also, at the same time, increase the risk of data theft or misuse of individual information.

User cooperation

When biometrics is deployed in settings where the aim is to identify individuals that have been categorised as 'dangerous' (e.g. individuals on the FBI's list of terror suspects), then a key limitation of most contemporary biometrics is that they often require a considerable degree of user cooperation. It is, for example, very difficult to capture an iris image of sufficiently good quality (for subsequent matching) if the individual whose iris is being captured is not in close proximity to the iris camera. This limitation represents a significant problem in these applications that aim to identify 'dangerous' individuals who, almost by definition, cannot be expected to cooperate and whose biometric data will therefore be difficult to capture. Yet, at the same time, it is necessary to capture their data in order for the biometric technology to perform a search that will alert security personnel, for example when the suspect is in a specific location (such as an airport). In other words, in some application contexts the promise of security through biometric technology depends upon a capacity to recognise identified 'suspects' from a distance. Now, a number of recent

technological developments have addressed this critical limitation and technology producers have declared that: 'iris recognition at a distance' will soon be a reality (Business Wire 2006).

This producer's statement has, however, been challenged. Considering the results from a large-scale deployment in the United Arab Emirates, an article in Biometric Technology Today, for example, concludes that: "iris at a distance is not yet mature enough" (Biometric Technology Today 2009: 2). Other recent developments have also been encouraged by this desire to overcome the challenge of user cooperation. One example is the amount of research on 'gait recognition' (Global Security Intelligence 2012; Toft 2004), a type of biometrics that ideally will enable the recognition of 'suspects' from a distance (Georgia Institute of Technology, 11 October 2002). This technology might be able to overcome some of the difficulties that other biometrics confront regarding the need for user cooperation. However, these efforts at countering technological limitations arguably bring about a new set of political concerns. In this case an example is the concerns that have been voiced about the potential misuse of covert biometric recognition. To illustrate the importance of this concern, it is worth noticing how the Office of the Privacy Commissioner of Canada (under Privacy Commissioner Jennifer Stoddart) recently stated that: "one concern is the covert collection and use of biometric data" (Office of the Privacy Commissioner of Canada 2011).

Template ageing

Another critical limitation to the promise of security through biometric technology is the problem of 'template ageing'. Template ageing refers to the issue of biometric recognition technology not being able to recognise and match the live biometric (e.g. the live fingerprint) of a person with a biometric of the same person taken at an earlier stage. This issue – that an individual's biometric (e.g. fingerprint pattern) might change over time – is problematic because the promise of security though biometric technology relies heavily on the assumption that once enrolled and stored a person can then be recognised forever after. This is a critical limitation in biometric systems, whose claim to deliver security is premised upon the ability of biometric recognition systems to determine whether the live biometric data of a person matches any of the templates in an existing database (e.g. of terror suspects). Indeed, this premise is severely compromised if the system fails to determine such a match simply because an 'aged' biometric template can no longer be recognised as matching the live fingerprint of the person from whom the template was originally collected. To minimise this limitation, iris

recognition technology has gained prominence, since this is a type of biometric information that is less likely to change over time (Tistarelli and Nixon 2009; Bowyer 2011). Yet two things must be noted. Firstly, that there are still challenges, such as cataracts, which will affect the use of iris recognition technology. As noted in a paper from the SANS Institute: "Subjects who are blind or have cataracts can also pose a challenge to iris recognition" (Khaw 2002: 9; see also LSE 2005).

Second, the process of matching is more difficult when using iris scans rather than fingerprints, given that most existing databases contain fingerprint templates and not iris images, which means that no or minimal matching against existing database entries or watch lists is possible. Crucially, this is a limitation that compromises the promise of greater security through the introduction of biometric technology in general as well as in efforts aimed at overcoming this particular issue of template ageing.

Scalability

There are two types of biometric recognition. One is the so-called 'one-to-one match' in which the purpose is verification of a person's claimed identity. The issue here is to verify (or reject) the reliability of the proclaimed identity. In this biometric recognition process the system is informed about the person's proclaimed identity such that it only pulls out the data file related to that identity (be it a set of fingerprint images, iris templates and/or facial photos). If this produces a match, then the biometric system will return a positive response to indicate that the person is who he or she claimed to be. If not, the system returns a negative response, indicating that the person does not match the data registered for that proclaimed identity. This process is referred to as a 'one-to-one' match. The other type of biometric recognition is identification, which is necessary when you are trying to identify a person that you don't know anything about. If you have a database of biometric fingerprint templates of numerous people and you have to identify an 'unknown' person then you can use biometric recognition to do this by taking, for example, a fingerprint from this person and feeding it into your biometric system. The system will then compare the fingerprint image with all entries in the database and tell you whether any of the existing entries match that of the person you are trying to identify. This is a 'one-to-many match' where the biometric system compares one biometric image (e.g. a fingerprint) with all fingerprint templates in the database in order to search for a match that can establish the identity of the otherwise 'unknown' person.

The reason that it is important to know of the difference between these systems is that where biometric systems are designed to perform 'one-to-many matches' it is necessary to be aware that the reliability of the performance of such systems will be limited depending on the size of the database being searched since the risk of making a false match will increase as the size of the database increases – as Lawrence Nadel notes: "Biometric system scale and performance are inversely related. For example, a system's false non-match rate (FNMR) is linearly proportional to the size of the enrolled database." (Nadel 2007: 2) One of the reasons that critics have called attention to this scalability limitation is that a crucial point about biometric security is the promise of automated recognition of individuals. However, the greater the number of false matches that are being made, the greater the need for 'human intervention' (to determine whether a match is a true or a false one and to make corrections accordingly). As such, it is a vital limitation that whenever the size of the biometric database increases so too does the likelihood that the technology might make a false match when asked to search the entire database. This is also why Whitley and Hosein have recently concluded about the performance of large-scale biometric systems that: "technological challenges here are significant and increase dramatically with the size of the population." (2010: 212) In short, the issue of scalability and performance still represents a crucial challenge to the promise of greater security through the implementation of large-scale biometric systems – and a challenge that is vital for policymakers to consider when making decisions about how and where to deploy biometric recognition as the solution to variously defined threats to contemporary security.

Interoperability

An important point about biometric recognition systems is that not only are there many different types of biometrics (fingerprints, iris patterns, etc.), there are also a great number of technology providers that often use different matching algorithms and different methods to translate biometric features into digital templates. The reason this is important is that insofar as the security function of a biometric system depends on being able to search different databases for a possible match, this function might be hindered if the different biometric templates are not able to interoperate because they conform to different standards (U.S. GAO 2011). For that reason, it has recently been stressed that: "one of the biggest challenges for biometrics involves the development and implementation of standards" (Stelter 2010). Indeed, this is also an issue that the U.S. General Accountability Office (GAO) has pointed out in a report that highlights the need to look carefully at the issue of interoperability. Specifically, the report notes that an insufficient adherence to biometric standards implies that

systems are not interoperable and that the biometric records that are being collected at various points consequently "cannot be searched automatically against the FBI's approximately 94 million." (Chabrow 2011; U.S. GAO 2011) As Lawrence Nadel has also noted: "significant advances continue to be made in biometric technology. However, the global war on terrorism ... has created the societal need for large-scale, interoperable biometric capabilities that challenge the capabilities of current biometric technology" (2007: 1). In 2011 Kevin Mangold from the U.S. National Institute of Standards and Technology identified the issue of establishing common standards for biometric data as the 'pre-eminent challenge' hindering effective system interoperability (Mangold 2011) and thereby limiting the promise of superior security. A 2006 report from the U.S. National Science and Technology Council's subcommittee on biometrics also pointed to the issue of system interoperability as one of the key challenges to the deployment of biometrics as a defence technology (2006: 14). However, even if standards were developed and implemented such that biometric data could be exchanged flawlessly, we still should be cautious about the promise of biometrics to deliver superior security (and the keenness of policymakers to embrace this promise).

Now, even if all five of these technological limitations were to be overcome, the context in which biometrics are being deployed entails two types of agency that are always present in any real world deployment context – and the reason that both of these types of agency are crucial is that they too may present limitations to the promise of biometric security that need to be taken seriously.

Contextual Limitations

Although knowledge of technological limitations is crucial when making decisions about how and where to deploy biometrics as a security technology, it must at the same time be said that knowledge of the technology in 'isolation' is not sufficient – it is indispensable also to pay careful attention to the context in which the technology is deployed. This section calls attention to two particular aspects of any deployment context that it argues are of utmost importance: namely *human* and *technological* agency (insofar as it makes sense to separate these). Notably, what becomes visible when we shift the focus of analysis in this way is that not only might the deployment of fallible biometric technology occasion a series of risks of which policymakers ought to become aware. More than that, even faultless biometric technologies might give rise to a different type of risk given the types of agency in the deployment context. Let me explain.

Misuse

The risk that even a flawless biometric technology might be misused necessarily represents a limitation to the promise that the introduction of biometrics will deliver superior security. Various critics have pointed to a number of important risks. It has, for example, been stressed that for most (if not all) biometric systems where data is stored in a centralised database there is an undeniable risk of unauthorised access to this biometric data. A crucial point about this risk is that it might translate into insecurity for those individuals whose data can now be accessed and "used for purposes that [they] would neither have predicted nor agreed to" (Alterman 2003). Consequently, this risk raises questions about the ethics of such biometric systems even when they are introduced in the name of greater security (van der Ploeg 2003).

Another important risk is that of data loss. This risk is often disregarded although numerous cases of the loss of sensitive digitalised data have already occurred. As one example amongst many, the Information Commissioner's Office (ICO) in Wales recently evaluated an incident where "five laptops and four memory sticks containing sensitive information have been lost by local [Welsh] authorities" – stressing that this is most regrettable given the risk that such data could end up "falling into the wrong hands" (BBC 2011). Hence human agency and the risk of data loss need to be taken seriously when deciding to deploy biometrics to advance security – if not, the effects might be extremely damaging for the individuals whose biometric data has been lost (Cavoukian 2009; Kumar and Zhang 2010).

In addition to the risk of data loss, it has also been pointed out that human agency brings about another possibility of misuse, namely the risk of 'spoofing'. Spoofing refers to the process by which individuals introduce a fake biometric sample (e.g. a fake fingerprint) to illegitimately bypass a biometric system. Such spoofing attacks undermine the integrity and security of a biometric system by introducing fake biometric data into the system. An example of spoofing would be the use of a fake biometric to fool a system into allowing access to 'secure space' by, say, presenting it with a copy of the fingerprint of a person who is allowed access. A worst-case scenario could be if a person on a watch list used the fake fingerprint of a person from a 'safe passenger' list to gain access, for example, to an airport. Experts have stressed that it is a misconception that fooling biometric systems in this way is almost impossible (and therefore needn't receive much attention). As explained by Stephanie Schuckers (associate professor of electrical and computer engineering at Clarkson University): "biometric devices are prone to 'spoofing' or attacks designed to defeat them" (Mahoney, 2006). Specifically, Professor Schuckers explains how "fake fingers moulded

from plastic, or even something as simple as Play-Doh or gelatine, can potentially be misread as authentic." (Mahoney, 2006; see also Thalheim et al. 2002; Kanellos 2005; van der Putte and Keuning 2000; Matsumoto 2002) Thus when a biometric is forged this process in itself entails a serious risk of illegitimate access to the very systems and spaces that the technology is believed to make 'safer' by presumably eliminating unwarranted access. Indeed, this risk of spoofing – and its potential consequences – is not simply a 'Minority Report' fantasy, but an issue that must be taken seriously as a practice that, as Bori Toth (biometric research and advisory lead at Deloitte & Touche) warns, is "turning from science fiction to reality" (Ranger 2006). Crucially, this risk not only compromises the security of the system but also that of the individual. If a person's fingerprint is spoofed this creates serious problems for the implicated person who cannot simply cancel his or her stolen fingerprint and order a new one (as when, for example, a bank card or a key is stolen). Referring to this point, critics have argued that the risk of having one's biometric feature(s) spoofed is a risk of a particularly serious kind insofar as it is irreversible (Meeks 2001).

Finally, it has been pointed out that even flawless biometrics might be misused politically, e.g. when biometrically derived 'knowledge' about an individual is presented as a scientific and unobjectionable truth in ways that hide from view what van der Ploeg refers to as the "normative aspects of automated social categorization" (van der Ploeg 2005) such that it becomes increasingly difficult to object to policies that embody what some would regard as objectionable normative aspects (such as racial or gendered categorizations). Indeed, as Shoshana A. Magnet points out in her recent book: "biometric discourse admits that racial profiling is occurring" (2011: 23) – and crucially, when pondering the risks that even faultless biometrics might give rise to, it is vital to bear in mind how such racial biometric profiling could be used in ways that would not necessarily increase the security of individual subjects.

The agency of biometric technology

Another limitation to the promise of biometric security can be discerned when we consider not only the human agency in any context but also the agency of technology (Latour 1992). On the one hand, the idea that biometric technology will deliver increased security relies on the assumption that profiling can take place automatically and at a speed that far exceeds what any human being could perform. This technological capacity is believed to deliver security because of how it presumably enables analysis of far greater amounts of data than human beings could process and with the vast amounts of biometric data being collected this capacity is necessary in order, for example, to recognise potential threats in databases containing millions of entries or in

airports with millions of people being 'processed' every day. In what follows it will be suggested that this kind of limitation can best be understood by considering the ways in which the technology embodies a sense of agency. An example of this is the way in which the technology (more specifically, advanced forms of pattern recognition) produces predictions about an individual's presumed 'future becoming'. Crucially, these predictions are sometimes regarded as a new type of knowledge about a person's becoming – a phenomenon that Mireille Hildebrandt refers to as 'profiling into the future' (Hildebrandt 2007).

For our purposes, what is crucial to note is the politics surrounding this constitution of a new type of knowledge and the implications for security when this knowledge feeds into politics. It is, for example, critical if these predictions are mistaken for knowledge that then forms the basis for political decisions that may deny a person rights that he or she is otherwise entitled to. Certainly, it is also worrying that these types of profiles are often invisible to the persons to whom they are applied and, therefore, impossible to correct if they are mistaken and/or illegitimate. To convey this point, Hildebrandt has introduced the term 'invisible visibility' to denote how, on the one hand, these predictions (and the algorithms through which they are derived) are invisible whilst, on the other hand, when these predictions are mistaken for unyielding knowledge and acted upon accordingly they then become visible in their consequences. Indeed, Hildebrandt argues that: "invisible visibility ... creates the possibility for sophisticated social sorting, requiring concern for illegitimate discrimination" (2009). In this sense biometric profiling contributes to the emergence of a new type of politically relevant body insofar as an additional aspect of human existence is opened up to profiling and political intervention. Put differently, in the relations that are established between biometric technology and the body to which it is addressed, a novel kind of body emerges as a new aspect of human existence (i.e. one's future becoming) and it simultaneously becomes accessible and assessable (Lindskov Jacobsen 2011). As Irma van der Ploeg notes about this development: the body changes as the biometric registration makes it 'machine-readable' (van der Ploeg 1999). In this process we see the emergence of a new conception of what aspects of human existence are open to intervention: only once the body's biometric data is registered does it become possible to think of a person's 'future becoming' as open to intervention and regulation.

This becomes possible to imagine because the biometric data (that ultimately make up this machine-readable body) can be analysed through processes of data mining that are thought capable of delivering a new type of knowledge about a subject's

future becoming (Hildebrandt 2007). In short, a new type of body emerges in the sense that previously inaccessible aspects (a person's becoming) are made 'visible' to a new science and rendered open to intervention by a new type of power. Various critics have alluded to related problems including the potential for governments to intervene in new aspects of human existence (Lindskov Jacobsen 2010), the insufficiency of existing data protection legislation to offer security to individuals in the face of this tendency (Hildebrandt and Gutwirth 2008) and the implications of this for democracy (Rouvroy 2008).

A critical point to stress here is that when considering how technology has agency, we can begin to understand how the use of biometrics can only be responsible insofar as it strives to consider how this technology may alter our very conception of what counts as a politically relevant and legitimately intervene-able type of body (Latour 1992; Introna 2007). Crucially, it is only once we recognise the sense in which biometric technology embodies a kind of agency that impacts upon our very conception of what counts as a political body, that we can begin to grasp an additional aspect of how the use of biometrics might have important implications for the promise of security – not only for bodies that faulty biometrics fail to register and that consequently become 'disqualified' (Muller 2004) but certainly also for those individuals that, in their capacity as newly machine-readable bodies, have come to be regarded as legitimate targets of political intervention.

By way of summary, the point of this section is not to say that instead of biometrics we should rather deploy this or that alternative technology – or no technology. Rather, the important point to be emphasised is that in order to deploy the technology responsibly – i.e. in a way that takes seriously the risk of engendering new insecurities – it is absolutely vital not only to be aware of the technical limitations of biometrics as discussed above, it is also vital to remain attentive to these two types of agency and the ways in which they, in a specific context, affect a certain deployment of biometric technology in ways that may not necessarily buttress the security of the individual whose biometrics are being registered and processed in the name of superior safety.

More specifically, responsibility in the face of the first contextual limitation (i.e. the risk of misuse) requires strong privacy protection measures – including system design principles such as data minimisation and encryption (see, for example, Ann Cavoukian 2011), policies on data-sharing, retention period and purpose specifications. However, responsibility in the face of the second kind of limitation (technological agency) might require a novel approach to issues of ethics and morality – one that

does not assume that the ethics of a technology deployment can be established before the actual rollout. Rather, it will require careful consideration of how the technology might affect the very objective of security that it is deployed to attain but which its real world usage might affect in ways that cannot be established a priori. This is a point that I will return to in the conclusion, but first the following section shifts the focus of the analysis from this explanation of various limitations to an illustration of how biometrics as a security technology is (nonetheless) expanding.

PART TWO: EXPANSION

Biometrics as an anti-terror technology

Whilst the use of biometrics has a long history it is, however, only fairly recently that it has come to be defined and deployed as an important security technology by the military. When the U.S. Army's biometrics programme started in 2000, its main focus was to determine how to use biometrics as a way to secure access to military networks. After the events of 11 September 2001 biometric technology then began to be deployed as a solution to various threats to security. Most notably, biometrics was quickly deployed as a new and much needed anti-terror technology (Rosenzweig, Kochems and Schwartz 2004). Biometrics was introduced at a number of U.S. ports of entry (notably in airports) to establish the 'true' identity of foreigners wanting to enter the U.S.: "In the Enhanced Border Security and Visa Entry Reform Act of 2002, the U.S. Congress mandated the use of biometrics in U.S. visas" (U.S. DOS 2012). Indeed, as van der Ploeg has also pointed out: "Vendors of biometrics were falling over each other to promote their products as the solution to the extremely heightened demands for security improvements, in particular at airports and other points of entry" (2005: 4). That the use of biometrics as a security and defence technology was new is also evident if we look at how research projects carried out at the U.S. Army War College began to engage questions aimed at "identifying the role that the Department of Defence and its Biometric Management Office should play in the emerging Homeland Defence organization" (Janker 2002). Indeed, some of these projects concluded that biometric technology was not so much a choice but, rather, a necessity in the face of the new threat of terror. This can, for example, be seen in a Strategy Research Project on "United States Homeland Security and National Biometric Identification" produced by Colonel Janker from the U.S. Army War College. In this report Janker states that: "Our willingness to prepare for further terrorist operations by implementing appropriate biometric identification systems within the United States will determine the impact and success of future terrorist acts".

This application context was then expanded as the U.S. Department of Defence recognised that biometrics could be used "to prevent the enemy in Iraq and Afghanistan from hiding behind a web of multiple identities" (U.S. DOD 2009b). Indeed, it has been noted that the U.S. "displayed the greatest urgency to use the technology following the 11 September 2001, terrorist attacks" (Visiongain 2008). And as a report from RAND Corporation also states: "biometric-based systems will become increasingly

important tools for identifying known and suspected terrorists. One tool to counter the threat of terrorism is the use of emerging biometric technologies" (Woodward 2001). Subsequent military and security engagements in Iraq and Afghanistan have reinforced this and, according to Dr Myra Gray, director of the Biometrics Task Force, what he refers to as 'biometric solutions' is the key technology that enables the Department of Defence "to identify and detain suspected enemies and terrorists" thus "improving citizen security both home and away" (U.S. DOD 2009b: 24). In other words, post 9/11, biometrics was quickly looked upon as a key 'anti-terror' technology. As the U.S. Department of Defence (DOD) also notes: "DOD senior leadership has recognized the important role that biometrics play in prosecuting the global war on terrorism, protecting our troops, and securing national security interests" (U.S. DOD 2009b). Thus, biometrics soon came to serve a key function in post 9/11 military operations on foreign territory. Indeed, it has recently been noted that: "The Department of Defence is the biggest user of biometrics outside the Department for Homeland Security" (Gold 2010: 7). As Steve Gold notes about the use of biometrics by the U.S. military: "the use of biometrics in military circles has increased significantly in recent years" (2010: 7).

As such, the use of biometrics as a security technology has expanded rapidly. As of 2004, the U.S. military started deploying biometrics in Iraq: "The concept of expanding biometrics for wholesale application on the battlefield was first tested in 2004 by Marine Corps units in Falluja, Iraq" (New York Times 2011). In Iraq, biometric technology (mainly fingerprint and face recognition) was introduced on the assumption that it would assist military personnel in the field in Iraq as well as intelligence services back in the U.S.. Yet, at the same time, it has been noted that: "there are times when biometrics can cause more problems than it may be worth" (Gold 2010: 7). An example of such a problem is that after U.S. soldiers in Iraq had collected vast amounts of data on civilians that they encountered, it was subsequently discovered that the databases storing this biometric data were not interoperable, which meant that database searches could not be performed as expected and, consequently, the enrolled persons could not be matched against existing databases in an attempt to determine whether one or more of them was a 'known' identity. Reiterating the problems associated with this issue of interoperability, a 2008 report from the U.S. Government Accountability Office (GAO) recommended that the Department of Defence should: "establish more guidance for biometrics collection" (U.S. GAO 2008). Having learned such lessons from the use of biometrics in Iraq, military deployment of biometrics was then moved on to Afghanistan (U.S. DOD 2009b). According to journalist and technology specialist Steve Gold, there are two main biometric projects

in active use in Afghanistan (2010). The first biometric project uses fingerprint readers, iris scanners and digital cameras to capture biometric information on detainees and what NATO refers to as 'other persons of interest' and, according to Gold, this project has "generated more than 400,000 sets of biometric data in its 18 months of operation" (2010: 7). The second biometric project is the Afghan Automated Biometric Identification System (AABIS), which has been developed, by NATO and the U.S. Department of Homeland Security (DHS) in close co-operation with the Afghan National Army. This project collects fingerprints and facial biometric data from army and police applicants. "According to NATO, the aim of this programme is to monitor movements of militants around Afghanistan, as well as keep Taliban infiltrators out of the Afghan army" (Gold 2010: 8). To this effect, the data captured in the field is collated and used in real time and then "relayed to Kabul where it is stored centrally and replicated to other databases across Afghanistan and back in the U.S." (Gold 2010).

Given that the implications of using biometrics as an anti-terror technology is an issue that has already been explored fairly extensively, the primary focus of this paper is not so much to add to these analyses but, rather, to use this literature as the background against which to analyse what I see as a shift in the use of biometric technology, a shift that has thus far received very little attention. Picking up on a phrase introduced by Benjamin Muller in his analysis of biometrics as a security technology, I will now turn to an exploration of how contemporary states' "obsession with technologies of risk" (2008: 199), including biometrics, has shifted in the sense that this obsession has now come to inform key initiatives in what has emerged as a new area of security policy, namely the fight against piracy off the coast of Somalia.

Biometrics as counter-piracy technology

> *"The Department of Defence (DOD)'s reasons to collect biometric data continuously change as DOD's role evolves wherever military operations are under way* [sic]*; whether in a desert environment fighting insurgents or on the high-seas* [sic] *fighting piracy."* (U.S. GAO 2011:6)

Biometric technology was deployed for the first time as an anti-piracy technology in 2009 by international naval forces patrolling in the sea off the Horn of Africa. Seaborne piracy is not a new phenomenon – it has arguably existed for as long as the sea has been used for transporting valuables. However, piracy has recently come to be

defined as a threat to global security. A key part of the background against which this representation has emerged was a series of events off the Horn of Africa in late 2008, which brought the problem of contemporary piracy to the forefront of international attention. In September 2008 pirates seized a Ukrainian ship carrying battle tanks and arms to Kenya (New York Times 2008a) and in November pirates captured a Saudi tanker filled with crude oil, a Philippine chemical tanker (New York Times 2008b), and the Danish ship CEC Future (DR 2009) and then, in December 2008, pirates also fired on an American-owned cruise liner (New Yourk Times 2008c). It must also be said, however, that prior to these events numerous ships carrying international relief supplies had been seized by pirates off the coast of Somalia. In 2005, for example, a group of pirates hijacked a ship carrying relief supplies for survivors of the tsunami (The Guardian 2005).

This surge in piracy off the coast of Somalia spurred a multi-national effort led by the U.S. to patrol the sea near the Horn of Africa. However, despite the various efforts made to curb the problem of modern piracy most such measures have proved largely ineffective (see, for example, Gilpin 2009; Wallace 2010; Dutton 2011). It is in the context of this escalation of the problem of piracy in 2008, combined with the shortcomings and unintended side effects of existing security measures intended to handle the problem, that the recent turn to biometrics as an anti-piracy technology needs to be understood. A key aspect of the expectations surrounding the use of biometrics to buttress the effectiveness of counter-piracy operations is related to "problems the international community faces in prosecuting pirates" (Guilfoyle 2011: 16). It can, for example, be difficult to deliver sufficient proof in court that the person suspected of piracy was indeed intent on carrying out such acts. Biometric registration is believed to solve this problem: if international naval forces that take part in NATO's piracy mission collect and store biometric fingerprints from suspects that they encounter, then this might eventually serve as evidence of 'intent' if this person is captured again. In what follows I will illustrate in more detail how biometrics has recently been introduced as a counter-piracy technology and elaborate on the expectations surrounding the technology.

On 15 May 2009, the U.S. Gettysburg in the Gulf of Aden sent, for the first time, the biometric files of 17 suspected pirates to the U.S. for the purpose of conducting a search against the DOD ABIS (Automated Biometric Identification System). These submissions resulted in non-identifications, but each submission improved the tactical value of the DOD ABIS and the likelihood of linking individuals to previous encounters. This use of biometrics is crucial since it is hoped that a check against this

database will help determine whether a suspected pirate can actually be prosecuted: if there is a match then the person's identity (and any previous illegal activity) is thus confirmed and the person can be brought back, for example, to the U.S. with a much smaller risk that a trial will prove unsuccessful due to lack of evidence and, hence, with a significantly smaller risk that the person might then, following an unsuccessful trial, apply for asylum on the grounds that – according to human rights law – he cannot be send back to Somalia; a country at war.

Hence, as the U.S. Navy intensifies its anti-pirate operations in and around the Gulf of Aden, the Biometric Task Force (BTF) continues to receive biometric records of suspected pirates from U.S. ships. For, as has been noted, "The ability to quickly and accurately determine if an individual is in the DOD ABIS database may deter future pirate attacks" (DOD Annual Report 2009: 33). This instance was also mentioned in a recent report from the Executive Office to the President, National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management:

> "On May 15, 2009, U.S. Navy personnel sent biometric files to BIMA [Biometrics Identity Management Agency] on 17 suspected pirates enrolled during an anti-piracy operation in the Gulf of Aden and documented their suspicious activity. By biometrically linking activities to individuals, legal processes can consider previous actions and prosecute individuals to the fullest extent of the law. Additionally, the increasing use of forward deployed biometric systems that share data and deny anonymity, provides a continuous deterrent to pirate activity" (Mangold 2011: 8).

Similarly in another recent report on "Defense Biometrics" the U.S. Government Accountability Office (GAO) notes that: "DOD's reasons to collect biometric data continuously change as DOD's role evolves wherever military operations are under way [*sic*]; whether in a desert environment fighting insurgents or on the high-seas [*sic*] fighting piracy" (U.S. GAO 2011:6). In other words, the application of biometric technology is thus shifting from its initial deployment as an anti-terror technology to now being considered as a favourable 'solution' to the problem of piracy, notably the problems involved in the effective prosecution of individuals captured at sea and suspected of being guilty of piracy. As Andrew J. Shapiro (U.S. Department of State) put it in his keynote address on the topic of 'Counter-Piracy Policy' in March 2010:

> "We are also thinking about creative ways to maximise the effectiveness of prosecutions and to send a stronger message of deterrence to would-be pirates.

> Strengthening the evidence gathering process through the use of biometrics might be an option, allowing for more effective tracking of individuals previously stopped by naval forces for suspicious maritime activities" (Shapiro March 2010).

And as Lieutenant Todd Hutchins (Naval Surface Warfare Officer, U.S.) notes in his recent article on how to defeat Somali pirates: "Under the 'deter and disrupt' strategy ... 'catch and release' entailed boarding pirate vessels, throwing weapons overboard, confiscating grappling equipment, and *gathering biometric data before freeing the pirates*" (2011: 828, my italics).

In short, whilst biometrics was initially deployed as an anti-terror defence technology, its field of application has now expanded as it is defined as a useful defence technology in the fight against seaborne piracy. What this paper stresses are the implications of this expansion when keeping in mind the four limitations, the types of agency involved and the constitutive implications of the technology on the borders of the body that it is being applied to. For insofar as security technology has a constitutive effect on the subject to whom it is being applied, we should then expect this expansion in the use of biometrics as security technology to have implications on the pirate body it is applied to. More specifically, we should expect to see changes in the borders of this body with respect to the political use of this technology, as biometrics allows a new form of entry into and authority over the body and in that sense its boundary is redrawn with respect to the powers that can legitimately intervene in it in the name of security. This point will be further explored in when discussing what I refer to as the emergence of 'the digital pirate', but before the report turns to this point, it is necessary first to elaborate on two additional aspects of this expansion of biometrics into the domain of counter-piracy.

Also bearing witness to the importance attributed to biometrics as a key security technology in the fight against seaborne piracy was a statement released by Interpol in June 2009. In this statement it was formally announced that: "Interpol is compiling a database of fingerprints, photographs and other personal information on Somali pirate suspects to help fight piracy at sea" (Glouchester Times 2009). Central to an appreciation of how this new biometric Interpol database is expected to advance the fight against seaborne piracy is the issue of data sharing which is presented as a solution to the current problem of positively identifying the persons captured during anti-piracy operations. Or, in the words of Interpol's executive director of police services Jean-Michel Louboutin: "Without systematically collecting photographs,

fingerprints and DNA profiles of arrested pirates and comparing them internationally, it is simply not possible to establish their true identity or to make connections which would otherwise be missed" (Interpol 2009). This point is evident in how Interpol finds it important to stress in its statement that the information contained in the new database can "be accessed by any of the agency's 187 member countries" (Africa Watch 2009). As described by Interpol Secretary General Ronald K. Noble in a media release on 17 June 2009 biometric data collection, storage and sharing provide a solution to the, thus far, largely ineffective fight against seaborne piracy insofar as the technology can provide "the 'missing link' to fill the gap which currently exists between the arrests made through military interventions and any eventual prosecutions" (Interpol 2009).

In other words, key to the deployment of biometrics as anti-piracy technology is the issue of biometric data sharing given that the prospect of successfully prosecuting a captured pirate is inseparable from the question of whether the person can be identified and, crucially, this identification process requires that a biometric template has already been captured from this person at a prior point of 'enrolment' and stored in an accessible and interoperable database. Only then can a search be carried out and a positive match produced. So only if the person's live biometric data (fingerprint or iris scan) can be matched against a template in an existing database can the deployment of biometrics serve the purpose of positive identification – otherwise the technology can only tell us that the biometrics from the captured person does not match any data in existing databases, meaning that he or she is not a 'known' person. As such, this new Interpol database serves a critical function in trying to establish the 'true' identity of the individuals being captured during anti-piracy operations. Bearing witness to this is, for example, the work of the Contact Group on Piracy off the Coast of Somalia (CGPCS) - a forum for exchange of information and ideas, and coordination of the efforts of states and relevant organisations through five working groups.

A critical example of the significance of such 'exchanges of information and ideas' is the relationship between Interpol and the EU concerning the issue of anti-piracy. Under the heading 'Information Sharing Implemented', the CGPCS describes how "following the European Council Decision 2010/766/CFSP, data collected by members of Operation Atalanta to identify suspected pirates will be shared with Interpol and checked against Interpol's databases" (CGPCS 2010). And the text on the website then further specifies that "the personal data used to identify suspected pirates include fingerprints, name or alias, date and place of birth, nationality, identification documents and personal data" (CGPCS 2010). Additionally, an information sharing

and analysis agreement between Interpol and Europol, including a working group to conduct analyses of maritime piracy data, was established in 2009.

It is important to stress that this shift in the deployment of biometrics from an anti-terror to an anti-piracy technology is not just a U.S. phenomenon. Indeed the issue is being debated far more widely. At a recent conference on Maritime Security held in April 2011 and organised by the UK-based International Centre for Parliamentary Studies, the use of biometrics in counter-piracy operations was discussed under the heading "Future Solutions to the Problems of Somali Piracy off the East African Coast". Representatives from the UN (Mr Augustine P. Mahiga, Special Representative for Somalia and Head of the United Nations Political Office for Somalia) and from the EU (Major General Buster Howes OEB, the Operational Commander, European Naval Force Somalia) among others, were invited to speak on the topic of "Port Security and Biometric Advances". Also in 2011, the Danish Ministry of Justice established a working group with representatives from the Danish defence forces, the national police and the public prosecutor's office. The working group was charged with producing a set of guidelines for the Danish naval vessels on how to handle cases that may result in prosecution of pirates in Denmark.

Key to the context within which this working group emerged was also the above-mentioned recognition and concern about how the lack of evidence hinders anti-piracy operations. As the final report notes:

> "As is the case for other types of crime, it is crucial that there is sufficient evidence to conduct a successful criminal court case. It is assessed that in the cases of many of those who are released, it is because such evidence does not exist. The guidelines are under preparation and the working group is currently investigating the possibilities for exchanging information, including biometric data, between the Danish defence forces and the Danish police in order for the police to be able to pass on the collected data to Interpol, which is responsible for the international coordination of prosecution, including that of individuals and groups who, through financing or otherwise, are supporting parts of the piracy activities off the coast of Somalia" (Danish Foreign Ministry 2011: 20–22).

What must also be said is that the introduction of biometrics into anti-terror operations is only one example of the expanding use of biometrics. This expansion in the application of biometric technology has, for example, also been alluded to by the

Canadian Privacy Commissioner Jennifer Stoddart, who notes that: "The Canadian government is expanding its use of biometrics" (Office of the Privacy Commissioner of Canada 2011).

Concluding remarks

Following the events of 11 September 2001, security issues related to the emerging desire for new identification processes have been raised to the highest level of priority. This has fed into a strong demand for high-tech solutions that promise to deliver faster and more reliable identification of individuals and, more specifically, biometric technologies have been looked to as an important part of such a 'solution'. As the above sections demonstrate, the expansion of biometrics as a panacea type solution to security issues is problematic. The technology is fallible in a number of critical respects that policymakers need to acknowledge have an impact on the ability of biometrics to deliver on the promise of superior security. Now, what also becomes clear is that besides these technical issues, there are two additional aspects that challenge the biometric security promise – two different sources of agency. First, biometrics can deliver insecurity (rather than superior safety) if humans deploy it maliciously. Second, if we reconsider the commonplace conception of technology simply as a means and embrace the argument that technology also has some potential for agency (Latour 1992), then it follows that the use of biometrics might also generate insecurity as a result of how the agency of the technology materialises when deployed in a specific context. In other words, even if biometrics are performed flawlessly there are still two reasons why expanding the use of this technology should be considered very carefully, bearing in mind these two additional sources of insecurity, namely human and technological agency; i.e. biometrics is expanding but at the same time there is a risk that these expanding uses of the technology fail to take seriously both the technology's limitations and fallibility and how deployments of the technology might generate new forms of insecurity. This is worrying and politicians should apply biometrics with a greater awareness of these critical issues.

Given the breadth of the possible issues involved in the implementation of biometric identification systems, this report recommends that it is important that resources are made available to facilitate continuous research that can advance our knowledge not only about technological developments in biometric profiling techniques, biometric database creation and use, but also about the societal, political and ethical implications of such technological developments and applications (see also van der Ploeg 2005). It is vital that we gain a better appreciation of the ways in which the development and deployment of biometrics as a security technology impacts upon contemporary political subjectivity, given the potential of biometric systems to alter the power balance between individuals and authorities. Only if we continue to expand our

knowledge of these issues may we be able to deploy biometrics responsibly – that is, in ways that do not compromise the rights of individuals. And to that end, it is also vital that system operators and authorities that form judgements about the safety (or not) of an individual do not trust blindly in the results of biometric identification, but remain critical. Moreover, given the likelihood of failure it is advisable that high priority is accorded to the implementation of measures that increase the possibilities for individual redressal (e.g. in cases where biometric identification processes make a false match). If the technology is trusted blindly and if there are no redressal mechanisms, simple technological failures can translate into insecurities confronting the very individuals that the biometric system is supposed to make safe.

Bibliography

Africa Watch (2009) "Interpol Compiling Somali Piracy Suspect Database", 17 June 2009

Alterman, Anton (2003) "'A piece of yourself': Ethical issues in biometric identification", *Ethics and Information Technology* 5: 3, pp. 139–150.

BBC (2011) "Council Confidential Data Loss Causes ICO Concern", BBC News Wales, 13 December 2011.

Biometric Technology Today (2009) "Iris at a distance not yet mature enough, says UAE", Vol. 17, No. 2, Feb. 2009.

Bowyer, Kevin W. (2011) "The results of the NICE.II Iris biometrics competition", *Pattern Recognition Letters* 33: 8, pp. 965–969.

Business Wire (2006) "Iridian Technologies Announces Improved Iris Recognition Algorithm", Moorestown, N.J., 3 May 2006

Cavoukian, Ann (2009) "'Privacy by Design.' The Answer to Overcoming Negative Externalities Arising from Poor Management of Personal Data" Trust Economics Workshop London, England, June 23, 2009, available at http://www.ipc.on.ca/images/Resources/2009-06-23-TrustEconomics.pdf3

Cavoukian, Ann (2011) "Patience, Persistence, and Faith: Evolving the Gold Standard in Privacy and Data Protection", *IFIP Advances in Information and Communication Technology* 354, pp. 1–16.

Chabrow, Eric (2011) "DoD Urged to Enforce Biometric Standards. GAO: Army Biometrics Collection Device Fails to Meet Standards", Data Breach Today, available at http://www.databreachtoday.asia/articles.php?art_id=3600

Contact Group on Piracy off the Cost of Somalia (CGPCS) (2010) "Oceans Beyond Piracy" From http://oceansbeyondpiracy.org/matrix/counter-piracy-activities-static. Website accessed on 21 May 2012.

DR – Danmarks Radio (2009) "Dealing with pirates". DR Documentary

Danish Foreign Ministry (2011) Strategy for the Danish Counter–Piracy Effort 2011–2014. http://um.dk/~/media/UM/English-site/Documents/Politics-and-diplomacy/Pirateristrategi_2011_ENG_WEB.ashx

Dutton, Yvonne (2011) "Maritime Piracy and the Impunity Gap: Insufficient National Laws or a Lack of Political Will?" Available at SSRN: http://ssrn.com/abstract=1931870 or http://dx.doi.org/10.2139/ssrn.1931870

Georgia Institute of Technology (2002) "Walk the Walk: Gait Recognition Technology Could Identify Humans at a Distance", *Research News*, 11 October 2002. From http://gtresearchnews.gatech.edu/newsrelease/GAIT.htm

Gilpin, Raymond (2009) "Counting the Costs of Somali Piracy", United States Institute of Peace (USIP).

Global Security Intelligence (2012) "Gait Recognition".http://globalseci.com/?page_id=44

Gloucester Times (2009) "Interpol Compiling Somali Piracy Database", 17 June 2009

The Guardian (2005) "Pirates Hijack Tsunami Aid Ship", 1 July 2005

The Guardian (2008) "Pirates take over oil tanker with British crew on board", 17 November 2008

Guilfoyle, Douglas (2011) "Towards a Robust Legal Framework on Piracy: Law and Politics". Paper presented at conference, Global Challenge, Regional Responses: Forging a Common Approach to Maritime Piracy, organised by the UAE Ministry of Foreign Affairs in association with DP World.

Gold, Steve (2010) "Military biometrics on the frontline", *Biometric Technology Today* 10, pp. 7–9.

Gray, Myra (2009) "Defending the US with biometrics", *Infosecurity* 6: 9, pp. 24–25.

Hildebrandt (2007) "Profiling into the future: An assessment of profiling technologies in the context of Ambient Intelligence", *FIDIS Journal*, Issue 1. From http://www.fidis.net/fileadmin/journal/issues/1-2007/Profiling_into_the_future.pdf

Hildebrandt (2009) "Who is Profiling Who? Invisible Visibility," in *Reinventing Data Protection?* (eds.) Gutwirth, Poullet, De Hert, De Terwaugne, Nouwt, and Dordrecht (2009). Springer.

Hildebrandt, Mireille and Serge Gutwirth (eds.) (2008) *Profiling the European Citizen: Cross-Disciplinary Perspectives.* Springer.

Interpol (2009) "Interpol member countries respond to calls to close the net on maritime piracy", Media Release, 17 June 2009

Introna, Lucas D. (2007) "Maintaining the reversibility of foldings: Making the ethics (politics) of information technology visible", *Ethics and Information Technology*. 9: 1, pp. 11–25.

Janker, Peter S. (2002) "United States Homeland Security and National Biometric Identification", USAWC Strategy Research Project. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA404488

Kanellos, Michael (2005) "Scientists pore over biometric-spoofing tests", *CNET News*, 22 December 2005.

Karacasulu, Nilüfer (2006) "Security and Globalization in the Context of International Terrorism", *Uluslararası Hukuk ve Politika Cilt* 2, No: 5 pp. 1–17.

Khaw, Penny (2002) "Iris Recognition Technology for Improved Authentication", *SANS Security Essentials (GSEC) Practical Assignment*, Version 1.3

Kumar, G. Hemantha, Mohammad Imran, Ashok Rao and R. Raghavendra (2010) "Multimodal biometrics: Analysis of handvein and palmprint combination used for person verification". Paper presented at conference, 3rd International Conference on Emerging Trends in Engineering and Technology, 2010, pp. 526–530. http://www.computer.org/portal/web/csdl/doi/10.1109/ICETET.2010.14

Kumar, Ajay and David Zhang (eds.) (2010) *Ethics and Policy of Biometrics: Third International Conference on Ethics and Policy of Biometrics and International Data Sharing*. Hong Kong: Springer.

Latham, Robert (2010) "Border formations: security and subjectivity at the border", *Citizenship Studies* 14: 2, pp. 185–201.

Latour, B. (1992) "Where are the missing masses? The sociology of a few mundane artifacts", in *Shaping technology / Building society: Studies in sociotechnical change,* Wiebe E. Bijker and John Law (eds), pp. 225–258, The MIT Press, Cambridge, MA.

Lindskov Jacobsen, Katja (2010) "Making design safe for citizens: A hidden history of humanitarian experimentation", *Citizenship Studies*, 14: 1, pp. 89–103.

Lindskov Jacobsen, Katja (2011) "Rethinking the 'bio' of bio-political security through humanitarian experimentation: the making of bodily boundaries and technological authority", Ph.D. Thesis, Lancaster University, Department of Politics and International Relations.

London School of Economics and Political Science (LSE) 2005. "The Identity Project – an assessment of the UK Identity Cards Bill and its implications." Department of Information Systems, the London School of Economics and Political Science.

Lyon, David (2008) "Biometrics, Identification and Surveillance", *Bioethics* 22: 9, pp. 499–508.

Magnet, Shoshana Amielle (2011) *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham: Duke University Press.

Mahoney, Patrick (2006) "Buddy, can you spare a ... finger?", *GlobalSpec Electronics*, 23 February 2006. From http://machinedesign.com/article/buddy-can-you-spare-a-finger-0223

Mane, Vijay Mahadeo and D.V. Jadhav (2009) "Review of Multimodal Biometrics: Applications, Challenges and Research *Areas", International Journal of Biometrics and Bioinformatics* 3: 5, pp. 66–95.

Mangold, Kevin (2011) "Biometric Systems and Interoperability". Paper presented at conference, Biometric Consortium Conferences, on behalf of National Institute of Standards and Technology.

Matsumoto, Tsutomu (2002) "Gummy and Conductive Silicone Rubber Fingers: Importance of Vulnerability Analysis", *Computer Science* 2501, pp. 59–65.

Meeks, B.N. (2001) "Blanking on rebellion: Where the future is 'Nabster' ", *Communications of the ACM* 44: 11, pp. 1–17.

Muller, Benjamin J. (2004) "(Dis)qualified bodies: securitization, citizenship, and 'identity management'", *Citizenship Studies* 8:3, pp. 279-294.

Muller, Benjamin J. (2008) "Securing the Political Imagination: Popular Culture, the Security Dispositif and the Biometric State", *Security Dialogue* 39: 2-3, pp. 199–220.

Muller, Benjamin J. (2011) "Risking it all at the Biometric Border: Mobility, Limits, and the Persistence of Securitization", *Geopolitics* 16: 1, pp. 91–106.

Nadel, Lawrence D. (2007) "Approaches to Face Image Capture at US-VISIT Ports of Entry", NIST Biometric Quality Workshop.

New York Times (2008a) "Somali Pirates seize Ukrainian Ship Carrying Tanks", 26 September 2008

New York Times (2008b) "Philippine Tanker Hijacked by Pirates", 11 November 2008

New York Times (2008c) "U.S. Cruise Ship Escapes Fire From Pirates in Gulf of Aden", 2 December 2008

New York Times (2011) "To Track Militants, U.S. Has System That Never Forgets a Face", 13 July 2001.

Office of the Privacy Commissioner of Canada (2011) "Data at Your Fingertips: Biometrics and the Challenges to Privacy", Ottawa, Canada. From http://www.i-gov.org/images/articles/15467/Biometrics.pdf

Pato, Joseph and Lynette Millett (eds.) (2010) "Biometric Recognition: Challenges and Opportunities. Whither Biometrics Committee; National Research Council. The National Academies Press.

Ranger, Steve (2006) "The Future of Crime – Biometric Spoofing?" Special to *ZDNet Asia* on 21 July 2006. Available at http://www.zdnetasia.com/crime-of-the-future-biometric-spoofing-39376855.htm

Rosenzweig, Paul, Alane Kochems and Ari Schwartz, (2004) "Biometric Technologies: Security, Legal, and Policy Implications," Heritage Foundation Legal Memorandum No. 12, June 21, 2004. www.heritage.org/Research/HomelandDefense/lm12.cfm

Rouvroy, Antoinette (2008) "Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence", *Studies in Ethics, Law, and Technology,* Berkeley Electronic Press, 2008.

Stelter, Leischen (2010) "Report finds biometrics 'fallible', but SIA disagrees", *Security Systems News*, Tuesday 23 November 2010, available at: http://www.securitysystemsnews.com/article/report-finds-biometrics-'fallible'-sia-disagrees - comment-form.

Strauß, Stefan (2011) "The Limits of Control – (Governmental) Identity Management from a Privacy Perspective", *IFIP Advances in Information and Communication Technology* 352, pp. 206–218.

Thalheim, Lisa, Jan Krissler and Peter-Michael Ziegler (2002) "Body Check: Biometric Access Protection Devices and their Programs Put to the Test", *c't Magazin für Computertechnik*, 11/2002, pp. 114ss. http://www.larc.usp.br/~pbarreto/Leitura 2 - Biometria.pdf

Tistarelli, Massimo and Mark S. Nixon (2009) "Advances in Biometrics", *Lecture Notes in Computer Science* 5558.

Toft, Dorthe (2004) "Forsvaret forsker i gangarter", *Computerworld,* 25 June 2004.

U.S. Government Accountability Office (GAO) (2011) "Defense Biometrics: DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies," Report to Congressional Requesters, GAO-11-276. March 2011..

U.S. Government Accountability Office (GAO) (2008) "DOD Can Establish More Guidance for Biometrics Collection and Explore Broader Data Sharing", GAO-09-49. 15 October 2008.

U.S. Department of Defense (DOD) (2009a) "Biometric Task Force", Annual Report FY 2009.

U.S. Department of Defense (DOD) (2009b) Annual Report Military and Security Developments.

U.S. Department of State (DOS) (2012) "Safety & Security of U.S. Borders: Biometrics". http://travel.state.gov/visa/immigrants/info/info_1336.html

U.S. National Science and Technology Council (NSTC) (2006) "The National Biometrics Challenge", August 2006, Washington D.C.

U.S. National Science and Technology Council (NSTC) (2011) "The National Biometrics Challenge", September 2011, Washington D.C.

Van der Ploeg, Irma (1999) "The illegal body: 'Eurodac' and the politics of biometric identification", *Ethics and Information Technology* 1: 4, pp. 295–302.

Van der Ploeg, Irma (2003) "Biometrics and privacy: a note on the politics of theorizing technology", *Information, Communication and Society* 6: 1, pp. 85–104.

Van der Ploeg, Irma (2005) "Biometric identification technologies: ethical implications of the informatization of the body", Biometric Technology and Ethics – BITE Policy Paper no. 1.

Van der Putte, Ton and Jeroen Keuning (2000) "Biometrical Fingerprint Recognition: Don't get your fingers burned", in *Fourth Working Conference on Smart Card Research and Advanced Applications*, pp. 289–303. Kluwer Academic Publishers.

Visiongain (2008) "Biometrics for Defense" 08/08/2008, Report by Visiongain. From http://www.visiongain.com/Report/327/Biometrics-for-Defence-2008

Wallace, Tye R. (2010) "Improving Counter-Piracy Operations in East Africa" Naval War College, Newport RI., Joint Military Operations Department. Accession Number ADA535303.

Whitley, Edgar A. and Gus Hosein (2010) "Global identity policies and technology: do we understand the question?", *Global Policy* 1: 2, pp. 209–215.

Williams, Martyn (2005) "Forget fingerprints and eye scans; the latest in biometrics is in vein", *International Data Group*. Available at: http://www.computerworld.com/s/article/102861/Forget_fingerprints_and_eye_scans_the_latest_in_biometrics_is_in_vein_the_latest_in_biometrics_is_in_vein

Woodward, John D. (2001) *Biometrics - Facing Up to Terrorism*. RAND Corporation. From http://www.rand.org/pubs/issue_papers/IP218.html

Woodward, John D. et al. (2003) *Biometrics: Identity Assurance in the Information Age*. Berkeley, California: McGraw-Hill/Osborne.

Zhang, Zhaoxiang, Maodi Hu and Yunhong Wang (2011) "A survey of advances in biometric gait recognition", in *Proceedings of the 6th Chinese Conference on Biometric Recognition* (CCBR'11), Zhenan Sun, Tieniu Tan, Jianhuang Lai, and Xilin Chen (eds.) Springer-Verlag, Berlin, Heidelberg, pp. 150–158.

Defence and Security Studies at DIIS

This publication is part of Defence and Security Studies of the Danish Institute for International Studies (DIIS).

The Defence and Security Studies unit focuses on six areas: Global security and the UN, the transatlantic relationship and NATO, European security and the EU, Danish defence and security policy, Crisis management and the use of force and New threats, terrorism and the spread of weapons of mass destruction.

Research subjects are formulated in consultation with the Danish Ministry of Defence. The design and the conclusions of the research are entirely independent, and do in no way automatically reflect the views of the ministries involved or any other government agency, nor do they constitute any official DIIS position.

The output of the Defence and Security Studies takes many forms – from research briefs to articles in international journals – in order to live up to our mutually constitutive aims of conducting high quality research and communicating its findings to the Danish public.

The main publications of the Defence and Security Studies published by DIIS are subject to peer review by one or more members of the review panel. Studies published elsewhere are reviewed according to the rules of the journal or publishing house in question.

Review Panel

Theo Farrell, Professor, King's College London
Daryl Howlet, Senior Lecturer in International Relations, Southampton University
Iver Neumann, Professor, Norwegian Institute for International Affairs (NUPI)
Norrie MacQueen, Head of Department of Politics, University of Dundee
Mehdi Mozaffari, Professor, University of Aarhus
Robert C. Nurick, Director, Carnegie Endowment for International Peace, Moscow
Mikkel Vedby Rasmussen, Professor with special responsibilities, Copenhagen University
Sten Rynning, Professor, University of Southern Denmark
Terry Terriff, Senior Lecturer, University of Birmingham
Ståle Ulriksen, Deputy Director and Head of the UN Programme, NUPI
Michael C. Williams, Professor, University of Wales at Aberystwyth
Clemens Stubbe Østergaard, Lecturer, University of Aarhus
Camilla T. N. Sørensen, Assistant Professor, University of Copenhagen
Bertel Heurlin, Jean Monnet Professor, University of Copenhagen