Realities of Biometric Surveillance

https://www.e-ir.info/2013/05/14/realities-of-biometric-surveillance/

ANDREW M. J. HUNTLEIGH, MAY 14 2013

Introduction

In 1998, futurist professor David Brin wrote a book discussing the inevitability of a heavily monitored and tracked society as a result of ever-rapidly advancing surveillance developments and increasing awareness of what could be done with such endless mountains of data; crucially, he also noted that states and citizens alike could benefit from such systems, and that efforts to balance these two competing uses were vital to protecting them both (Brin: 81). Though he did discuss legitimate security concerns as part of the push for the state to perpetually ratchet up surveillance, and even anticipated the day would inevitably come where calamity-based security concerns would possess the force to push other considerations aside (Brin: 87), he also discussed considerations about reasons to limit the technology and also about reasons to deploy the technology. Though surveillance comes in countless forms, one of its most persistently controversial methods is biometric identification. The nation-wide recording of biometric-like data has been advanced by some experts since at least 1934 (Watner & McElroy: 5), and whether looking at grade school lunch lines (Graziano: 1) or war zones (Baldor: 1), the modern popularity of biometric identification, thanks to its synergy of new technology, convenience, and security, is undeniable.

But it is an understatement to say that these advances are controversial—the relative ease with which such systems have proliferated belies the intense opposition to their very existence by many privacy and civil liberties advocates, and their human security concerns[1] represent very real potential exploitation by governments as these systems gained increasing presence and sophistication. The cameras slowly filling Manhattan (Honan: 1), or much of Britain (Travis: 1), represent a definite kind of paranoiac threat even now, knowing that someone is watching you but not who or why—but they would represent a very different kind of threat if each of them instantly recognized the observed's face, and could instantly display outstanding warrants (or traffic fines) to the observer, and potentially even automatically initiate appropriate measures. This is the future-reality of biometric identification.

Fundamental Concepts

Before going any farther, it is important to discuss the specific definitions of "state security" and "human security" used throughout this analysis are initially drawn from the same source, for ease of reference. State security refers to the Westphalian conceptualization of the state as the referent object for maintaining safety, created as nationalism gave rise to a communal identity largely subsuming the individual (MacFarlane & Khoong: 5-6). Human security, on the other hand, refers generally to the expansion of security concepts to include other subjects such as the economy, health, gender, welfare, and identity (Ibidem: 1). That said, the problem of human security covering everything and thus being analytically useless (Paris: 102, MacFarlane & Khoong: 240) is a legitimate concern. Related to this problem is the inherently contradictory idea of human security as protecting aspects of culture or identity for one group that directly threaten the culture or identity of other groups, such as using human security as a reason to liberate women from wearing Islamic headwear and thus reducing Muslim identity human security in turn (MacFarlane & Khoong: 13). Thus, this work's concept of human security rests on a conceptualization of protection of individual humans from organizations of other humans (Ibidem: 248); in other words, keeping the individual safe from both illegitimate government-led jailing or harassment as well as simultaneously keeping the individual safe from illegitimate terrorist-led violence.

In addition to the understandings of human and state security, it is also important to understand the attitudes of the supporters and the critics of dimensions of biometric identification systems. Human security supporters broadly come in two varieties, each with their own ideas about what defending the individual should look like: privacy advocates, who generally push for strong individualism, and communitarians, who support strengthening individuals through promoting the common good. This conception of a greater cause than the individual occasionally results in the communitarians supporting state security; ardent in their support for state security are the statists who suggest that the security of the country is good for the security of everyone within the country, representing the antithesis of concern regarding the individual. Voices from each viewpoint will help frame the issues they each find to be of particular interest, sometimes conflicting but often overlapping—which ultimately is the key to moving forward on the issue as a whole.

Problem

There is little doubt that both states and their citizens alike benefit from genuinely good security—at least four of the terrorists involved in attacking the World Trade Center and the Pentagon were stopped and questioned by law enforcement agents but ultimately released, despite each possessing a legal justification for arrest that remained unknown to the officers (Wang: 1). Thus, relatively minor increases in successful identification technologies may have thwarted their plans at least in part, and it goes without saying that both America and many of its citizens would have benefitted from such an increase in security. But such systems are not without their drawbacks. So what is the overall concern here? Surely "[i]f you've done nothing wrong/you've got nothing to fear" (BBC: 1)? One problem is that technology, generally speaking, is not known for being flawless. Whether human error torpedoes its data's successful deployment, human error creates errors in the data-entry process itself, or the system's design is fundamentally flawed, the outcome is the same: mistakes that are embarrassing at best and fatal at worst. An equally worrying problem comes, as privacy advocates remind us it so often does, when authority granted for using identification information for one purpose is used for another (Smith: 305)—and the problem is compounded when nothing is done about this misappropriation, and such behavior becomes standard operating procedure. It is easy to imagine a police department lamenting lack of access to a federal aviation database—and then discovering that, one major tragedy later, it has the impetus and even potential public support to justify setting up information-sharing deals.

Obviously, both state security and human security are vital concerns regarding the implementation and usage of biometric identification technologies in society—but while state security is a fairly obvious concept, what does "human security" have to show us for this analysis? Well, the threats biometric identification pose are not the kind that will topple states or destroy societies—those are the threats biometric identification seeks to help guard against. Rather, biometric identification represents threats of political repression, which falls quite easily in line with the United Nations' 1994 Human Development Report, clearly stating why this is so vital: "Human security is not a concern with weapons—it is a concern with human life and dignity" (UNDP: 22). But what are the privacy advocate, communitarian, and statist arguments for and against such technologies' usage for each locus of security? What kinds of biometric technologies are viable to use, are likely to be used in the future, and are generally best to use? Ultimately, all these issues are tied together, and the question must be posed as to how concerns of both state and human security can be addressed in cobbling together a workable solution for protecting their shared societies.

Biometric Identification Proliferation

Biometric identification's beginnings are far less modern than the futurist-sounding word suggests; perhaps the earliest form was the primitive mid-1800s Bertillonage system of standardized measurement-taking parameters (Parenti: 42), a painfully slow human-oriented undertaking that provided essentially the same sort of potential identification certainty that modern systems promise—unfortunately, the logistics of taking careful measurements of every air traveler's numerous specific measurement points (Parenti: 45) before they were allowed to fly sound particularly infeasible today. But, as in many areas of society, technological advancements have allowed solid-but-infeasible ideas to become ever-increasingly possible—and these kinds of possibilities appeal to states and private organizations alike, a kind of virtual guarantee of an advancement-and-implementation spiral.

Examples of biometric implementation before the World Trade Center's destruction are fairly limited—fingerprints had already been in wide use for over a century, and DNA analysis was the only other heavily used biometric identification technology, which was (and is) still impractical for rapid identification. Retina or facial scans were science-fiction mainstays, and technologies such as gait identification or heat pattern recognition had not even reached that level of public consciousness. Only a few years after 2001, all of these devices and more were beginning to enter the public discourse as awareness of the increased need of, and increasing general acceptance for, biometric identification systems became apparent (Jain, Ross, & Pankanti: 125); "there has been no higher priority for the United States than improving its homeland security so that tragic attacks like [the World Trade Center's destruction] might never occur again" (O'Hanlon et alia: vii). The International Civil Aviation Organization decided in 2003 that all machine-readable airline tickets should contain biometric information (ICAO: 1); Amsterdam's Schiphol Airport has had an iris-scanning system in place for years for its frequent flier program (Jain et alia: 130), and the United Kingdom uses a similar system at some airports, bragging how its registrants can cross the border in "20 seconds" (UKHOBA: 1); Iraq's biometric identification forays started when Fallujah effectively became a gated community run by identification cards and retinal scans (Peterson: 1); the Pictet & Cie bank in Geneva relies solely on such identification systems for internal checkpoint purposes (SMACS: 1); ordinary American grocery stores once implemented fingerprint scanners for ease of checkout (Hesseldahl: 1), but were probably just following Walt Disney World's lead for its season pass holders (Bogatin: 1)–and biometric identification is one of the few things that Disney World likely has in common with the average Las Vegas casino (Martin: 112). More modern cutting-edge biometrics research sets entirely new bars for fact-over-fiction, from the development of seats that can identify the biometric data of their occupants (Ferro et alia: 451), to the FBI's assistant director saying even as-yet-unused biometric data like scars, tattoos, and facial shapes are to be collected for future "plug-and-play" use (Arena & Cratty: 1)—to the compilation and reading of wrinkles around the human eye for imperfect retinal scans due to blinking (Clemson University: 2009), suggesting that such technology is fully intended to be used on unwitting subjects. This list is merely illustrative, but should serve to demonstrate the wide variety of situations in which such systems are already used.

These biometric scans fall into two major categories of gatekeeping: alerting authorities to the presence of a wanted individual and preventing unauthorized access to areas or activities. The key functions biometric identification plays can thus be seen as acting either as a "name" or a "password" (Brin: 236) to allow for recognition or access, respectively (though access also requires recognition). The importance of the function as a "name" is that unique identifiers such as biometrics can help alleviate the confusion when two identically-named individuals need to be differentiated, whether two Marys Q. Smith (Ibidem: 236) or T.s Kennedy. Privacy advocates would counter that, noble though this goal may be, a single database error can cause even greater problems (Garfinkel: 23) than a primitive non-biometric identity check might—but using the human body as a password (Brin: 240) holds significant potential to communitarians.

Issues of border security are paramount in preventing potential harm to both the government and to individual citizens—Alabama Senator Jeff Sessions called biometric identification technology in such environments the "best non-lethal defense against terrorism" (Baldor: 1). But depending on implementation, it can still lead to favoring one type of security over the other. Standard privacy advocate arguments regarding the problems of any surveillance regime suggest the favoring of state security goals over human security goals (Cook: 179)—but there are also serious problems for state security (and perversely for human security in turn) with letting human security completely set the agenda, particularly if the extremes of anonymity favored by privacy advocates were adopted, bringing decreased accountability overall (Brin: 199-200) and pushing more toward a society where communitarians and privacy advocates alike point out that corporations continue to exploit personal information (Etzioni: 131) with no concern to its accuracy (Smith: 313), while the government is unable to use such information for arguably more noble goals (Etzioni: 131), even if the reality of unjustifiable use remains troubling (Parenti: 200). With this in mind, the next section discusses how the statist viewpoint nonetheless promotes such technology.

State Security Versus Human Security

State security's interest in biometric identification systems seems a virtual given; "perimeter security at the country's borders" was listed first in the analysis of four primary strategic anti-terrorist initiatives proposed after a

comprehensive examination of state security failures in the World Trade Center's aftermath (O'Hanlon et alia: 3). Even before the appearance of the new worldwide terrorist threat, the Cold War drove the United States, the Soviet Union, and their allies, in an ever-escalating quest to create newer and better surveillance and tracking systems to identify potential enemy agents and generally obtain informational superiority (Smith: 97-99). These security-driven surveillance goals intensified incalculably after the destruction of the World Trade Center (O'Hanlon et alia: 4), and myriad developments the world over (such as those discussed in the introduction) see continual technology upgrades with the shared goal of guarding against unauthorized access—be it to entering a bank vault or to boarding an airplane. The statist argument remains essentially that it would be foolish not to take advantage of any new potential technologies that could assist with homeland security—wanting or needing something "worth [more] than a little extra privacy" (Gotlieb: 158), such as the protection of your entire society, certainly seems worth the trade-off. Privacy advocates counter that, regardless of the true goal, it is always a series of small privacy-reducing steps that lead irrevocably to tyranny (Watner: 103, 107, 112).

To the statist, the most obvious benefits that biometric identification represents to state security are increases in both the efficiency and the effectiveness of identification screening. Examining two countries in particular can best represent successful proofs-of-concept for the streamlining and cost-cutting of border security: Portugal has replaced many of its security lines with fully automated systems, claiming both that such lines move three times faster and can do the work of five security officers, and kiosks at Singapore's borders run by the NEC corporation claim to have cut migration time down to 12 seconds per person using extant e-passport technology linked to fingerprints, and specifically discuss future expansions of facial and iris recognition technologies, all without the aid of a single human operator (NEC: 1). Though costs are likely to initially be prohibitive for installing new security measures, demonstrated by the multi-billion-dollar rush to tighten controls nationwide after the World Trade Center's destruction (Harris: 1), over time these engines of increased efficiency and effectiveness could also help lower security costs for border controls.

Such security measures do not come without drawbacks, most frequently expressed by privacy advocates; seemingly the very moment a new biometric technology is announced, some group will claim that the technology is insecure and can be easily compromised. Any heavy reliance on technology for important purposes immediately invites attention from individuals looking for a way to demonstrate technological limitations—and whether these acts are done for personal gain or the public good, the result is similar. Public demonstrations of technological failings can only decrease public confidence in the technologies, and pushing these technologies despite their failings may result in the commonly-heard refrain that such systems are not good at catching criminals, but rather good at impeding the law-abiding populace who presumably will not work to circumvent the system—a sentiment expressed about identification systems commonly today by privacy advocates, but expressed (specifically about the passport) as early as 1858—by Napoleon III (Lloyd: 23), not long after a forged passport was found on his would-be assassin (Ibidem: 22).

General responses to state security concerns from human security spokespeople, such as the head of the American Civil Liberties Union's Technology and Liberty Project director, are generally clear and succinct: "thousands of mistakes have already been made with the use of so-called no-fly lists at airports—[and] giving law enforcement widespread data collection techniques should cause major privacy alarms" (Arena & Cratty: 1). Potential for future abuse by combining multiple systems is readily apparent, such as the merger of the extant satellite monitoring of traffic jams, combined with systems like SpeedPass and EZPass (Parenti: 126-127), then also merged with biometric identification systems already used for crucial border security to put together the ability for a government to easily ascertain the whereabouts of anyone engaging with public transportation in this way. This is actually similar to the systems employed in some Las Vegas casinos, as suspicious individuals can be tracked from one table to another while the camera operators stay in touch with both dealers and bouncers (Martin: 116). But the communitarians have a counter-argument for accepting the inconveniences of surveillance technologies—"anonymity is the darkness behind which most miscreants—from mere troublemakers all the way to mass murderers … shelter in order to wreak harm, safe against discovery …. [surveillance] can be irritating to the honest, but it is devastating to knaves and despots" (Brin: 215).

Drawbacks for human security are better publicized in news stories about biometric identification, so they can be

analyzed first—the dual problems of making mistakes and governmental overreach are paramount to most any discussion of biometric identification's problems to human security. Mistakes have a disproportionate impact on human security—the people, not the government, suffer from false positives, and false negatives are rarer simply due to the tiny minority of individuals actually intended to be caught by security initiatives. Even small failure rates, often glossed over as completely unproblematic by those espousing the benefits of biometric identification (Thomas: 1), can ruin a passenger's day, vacation, or personal life, adding to privacy advocates' arguments, though tempered for communitarians as per the above quote. The sort of machine-reading difficulties leading to false positives could lead both to greater general suspicion and a greater tendency to assume any positive is a false positive.

Regarding general human security concerns, privacy advocates are quick to point out that "the progress of science in furnishing the government with means of espionage … may bring means of exploring unexpressed beliefs, thoughts and emotions" (Smith: 151), though communitarians also arguing for peoples' rights argue that privacy advocates are "block[ing] the implementation of many policies and devices that could have profoundly positive impacts on the public good" (Etzioni: 7-8), or "[u]sing privacy as a shield … seek[ing] to freeze the world as they were accustomed to it—a slow-paced realm of quaint filing cabinets…" (Brin: 77) instead of acknowledging that individuals of all social classes in America have more freedom today than ever before, "despite the fact that our government knows far more about its citizens than any other in history" (Ibidem: 87). The statist view would simply point out that failing to use new technology and enforcing increasingly individual-centric satisfaction requirements may lead to less stringent and therefore less effective security (Lloyd: 257-258).

This sort of governmental overreach is a vague yet threatening problem for human security. Particularly in a society like the United States where nearly 1 in 100 adults is currently incarcerated (Liptak: 1), it is understandable that there is concern over the government's willingness to overuse its powers. If a technology can be put into place at borders or in airports or seaports, it could surely be used in other places. The scope of these "other places" is precisely the problem of implementation for human security, particularly for privacy advocates; if the system proves successful for one task, it will inevitably be tried for another task (Parenti: 179). It is entirely too common to focus on the relatively obvious drawbacks for biometric identification in human security terms, however; thus, a turn to some seemingly unheralded benefits for human security is in order, starting with a benefit dear to communitarians.

Racial profiling, widely condemned yet widely suspected, is seen as something of a necessary evil in those times when it is defended. Biometric identification has the noteworthy advantage of ignoring the problems of this system by sidestepping the concept entirely, and with much greater efficiency than would a policy advocating solely human-run individual scrutiny—fitting with the communitarian ideal that surveillance be fair and minimally intrusive (Etzioni: 13). Perhaps the inherent racist idea that all people of another ethnicity "look alike" could impact a security guard's judgment, but surveillance technologies know that everyone looks at least a little bit different[2]. Claims that this new system will result in the undemocratic practice of treating people as suspects merely because they are engaging in a certain activity likely ring hollow to minority ethnic groups who have experienced this kind of universal suspicion and lack of privacy (Brin: 69) since long before the days of retinal scanning. It will likely make a lot of people uncomfortable to no longer be above suspicion due to their majority or socio-economic status, and many privacy advocates oppose virtually all surveillance on the grounds that it is an "organization of the body into a standardized text to be read by the law" (Parenti: 42), but human security is benefitted by this flattening of discriminatory behavior just as much as is state security.

In Sum: State and Human Security Overlap

Throughout this section, the conflicting purposes of human and state security each seemed justified in the related concerns regarding biometric identification. Crucially, there are definite areas where the two concepts agree, and thus these are areas with greatest potential. The shared interest in detection of individuals intent on causing harm to citizens means mutual support for "perimeter security at the country's borders" (O'Hanlon et alia: 3) ties into the similarly shared interest in developing the most accurate and reliable systems possible in order to minimize false negatives, which of the two types of identification errors is the one with the most resonance to both sides. Similar to the benefits of reducing false negatives, increasing the speed at which such identification takes place is of interest to both governments and individuals, playing into ideals of efficiency and convenience.

Dueling Security Assurance Trade-Offs: Having and Also Eating One's Cake

The ultimate question for the future of biometric security, in light of these positive and negative aspects for each type of security, is an obvious yet important one: How is it possible to ensure that the human security aspects of biometric technologies prevail over the traditional security aspects, or at the very least attain parity? When presented with a situation wherein a suspect is identified as having potentially committed a crime, there are three fundamental choices: ignoring the evidence, jailing/executing the individual, or seeking to uncover the truth of the matter and judge which of the two is warranted (Etzioni: 95). In a sense, these paradigms represent, respectively, crude concepts of freedom, oppression, and justice. That liberal democracies supposedly since the time of the Magna Carta have made a special point of favoring justice, a "balanced" approach to security (Ibidem: 95), does little to dissipate the notion that states are still obviously prone to favoring their own security over the security of any given individual. Thus, state security can be seen as hinging on oppression by subsuming individual interests to the state (MacFarlane & Khoong: 6), in a similar way that human security hinges on the ability of the individual to remain free from the oppression of organizations (Ibidem: 248)—meanwhile, justice is not a free-standing concept, but rather is compatible with the other two. The question is what steps are taken to ensure that human and state security concerns are balanced in the pursuit of justice.

Unobtrusiveness

The concept of unobtrusive security helps illustrate a fundamentally important trait of any good security technology—it must uphold the inherent concept of a suspect being (and feeling) innocent until proven guilty. The basic logical error made by many biometric identification detractors is that such technologies will turn everyone in America into a suspect, therefore undoing the concept of innocence until guilt is proven. Unfortunately for these detractors, they are separating a single concept into two concepts: suspects *are* the individuals who are innocent until proven guilty, not that suspects are automatically assumed to be guilty. There is a reasonable concern, both from statist and communitarian viewpoints, to ascertain that individuals wanted for serious crimes are not eluding capture by assuming false identities. In order to use modern technologies to assist in such endeavors and eliminate human bias, everyone at crucial security checkpoints *must* be treated as a suspect, and—crucially—*thus* is presumed innocent until proven guilty. This level of intrusive surveillance may sound unpalatable, but ultimately is just an evolution of the already commonplace everyone-as-suspect scenarios of metal detectors at public venues or document checks at border crossings.

This is not to say that easing concerns over such technologies is unimportant—rather, it is very important to minimize both metaphorical and actual flashing lights and sirens. One of the most important fundamental considerations for both legitimately maintaining innocence of suspects and of keeping public fears minimal, thus finding common ground to privacy advocate, communitarian, and statist goals, is to treat every positive identification made of a *person of interest* as a potential mistake, no matter how sure the technology may claim it is. All due attention must still be paid to the alert, but no guns are drawn and no people are whisked away to windowless interrogation rooms for hours—those things can be part of the process, but there must first be a human check on the validity of the system's identification, which has the dual impact of reducing fears and avoiding needless escalation. This is particularly true in light of privacy advocates' reminder that biometric data, once stored in a computer, can be forged in the sense that it could be associated with a different file, either intentionally or unintentionally (Garfinkel: 65), and agrees with statist concerns that lax human checks will lead to lax security (Lloyd: 258) and thus human verification would be almost necessary—but not deploying biometric identification systems because they possess faults is questionable when the current system's faults could well be even greater.

Another important and not well-examined area for proper balance is the area of surveillance unobtrusiveness, as alluded to in the earlier discussion of innocence and guilt. Certainly, it is vitally important that the fear many individuals feel in relation to technological identification devices is mitigated in ways before the point of positive identification as well. Las Vegas casinos can serve as a non-obvious but substantially applicable model for much of the kinds of identification and tracking that are essential to border security; namely, the sort that is capable of extremely tight scrutiny of all coming and going individuals, yet remains completely unobtrusive unless a security emergency arises (Martin: 112-113). There is something to be said for "out of sight, out of mind" when designing

surveillance systems that are likely to be seen as Orwellian anyway. This is certainly a far cry from the clumsily and openly implemented no-fly list, which notoriously had such vague information that thousands of people were able to fit the positive identification of vaguely defined threats to aviation security (ACLU [2]: 1), and thus failed both at protecting the state and from illegitimately harassing the citizenry.

Unobtrusiveness has been largely ignored in biometric identification implementation thus far, such as in Portugal and Singapore as discussed above, though this is due in part to the particular choices made—fingerprints are hard to scan without an obvious sensor. But in Portugal's case, a facial scan is also processed, and rather than a casual scan while standing in line, the scan takes place after stepping alone into a clear glass box, which seems to be a needlessly terrifying futuristic addition to the surveillance experience. Alternatives, such as the non-obvious awareness programs used in Las Vegas casinos, already claimed a few years back to be able to process an individual's security history within seconds without alerting the individual of the surveillance (Martin: 116), thus the technology could prove to be a particular boon to security if used correctly and legitimately. That said, checking every traveller against a non-obvious awareness database such as those used at casinos would surely result in a cavalcade of false positives without carefully delineated concepts of what "hits" actually matter. With crime and incarceration rates being what they are, it seems likely that huge numbers of citizens would come up as connected to a felon or a felony; thus, in order to preserve relevant aspects of human security, the relevant positives would need to be limited to serious state security concerns such as terrorism and perhaps organized crime.

One important caveat raised by privacy advocates about large-scale unobtrusive surveillance is that its very non-obvious nature potentially renders it even more likely to catch individuals engaging in activities that, even if not illegal per se, the individuals would rather not have enter into public knowledge, and that furthermore there is then no specific person to hold accountable (Smith: 67). Governmental data collection proliferation efforts already seem driven to some extent by the 1984esque need to compile more and better data and check it faster for its own sake (Lloyd: 160-161); adding easier sources of potential blackmail to these systems could certainly prove embarrassing or worse in the hands of corrupt government officials.

Other Directions

A solution that may have a great deal of merit, particularly for privacy advocates, yet that never seems to arise even in these discussions, is the ability to opt-out from biometric identification at security checkpoints. If an individual is extremely uncomfortable with the idea, for whatever ideological or practical reasons, there is no good reason to deny that person a more thorough old-fashioned security check instead. Perhaps such individuals would come to expect that they may need to arrive at the airport yet another hour earlier than everyone else, or that crossing the border would take twice as long as it takes a less paranoid driver, but there is no reason to think the government could not indulge in these personal wishes. Better to have a formal system in place than to end up with people wearing enormous sunglasses, heat-blocking make-up, hunching over and refusing to speak in efforts to foil the biometric identification *du jour*. Statist and communitarian viewpoints also seem well in line to accept such a compromise.

Finally, in order to best balance state and human security concerns, the use of multiple overlapping forms of biometric identification could both maximize the chances of detection and minimize the chances of unnecessary harassment; even contributors to a journal heavily supporting the use of biometrics readily admit that "[n]o single biometric is expected to effectively meet all of the requirements (e.g., accuracy, practicality, and cost) of all applications" (Jain et alia: 126). There are already databases and plans in order, backed by at least $1 billion at the FBI alone (Arena & Cratty: 1), to initiate something called the "Next Generation Identification System" for seemingly this very reason (FBI: 1). In addition to the FBI's already enormous fingerprint database, this project adds the potential for overlapping iris/retinal scan and voice print data, in addition to potentially expanding further into whatever new technologies become feasible to implement (Ibidem: 1). Whenever there is a chance for error—and there is always a chance for error—it is necessary to have multiple checks in place, to act as safeguards. This can involve the checking of an individual against multiple levels of surveillance technology in turn, where even the unexpected false positive could be instantly nullified by other disagreeing systems, or even as simple as ensuring that there is a second level of human-based scrutiny on any false positive.

Accountability

Tales of individuals not knowing where to turn, feeling as though there is no recourse to fix their cases of mistaken identity, have abounded in recent American history, particularly in regards to the many problems experienced as a result of the American "no-fly list" (ACLU: [2] 1). Ted Kennedy made it a point to lambaste the fact that even with his enormous political influence, he was refused the ability to board on five separate occasions thanks to a no-fly list, and it took between his first delay in March and the fifth delay in April to finally get his name removed from the list (Goo: 1). The problems ordinary people could face in an environment where even the powerful are hard-pressed to work with the system (Ibidem: 1) demonstrate the need for a more efficient appeal system. The TSA's 2004 solution, sending a letter vouching for a person's innocence that the individual can show to the questioning authorities (Ibidem: 1) sounds suspiciously like a substantial security threat in its own right, showing the way in which one poorly-designed system can lead to a spiral of unfortunate consequences.

Any appeals system designed would need to be simple, responsive, and most importantly, have on hand its fair share of biometric identification whenever possible. If the infamous known criminal alias "T. Kennedy" (Goo: 1) has fingerprints, a photograph, a voice print, or any other such information available to authorities, then there should be a way of pairing this with the no-fly list in case of an appeal. The Transportation Security Administration itself could likely take on this new responsibility, though both running and overseeing no-fly lists would likely result in less accountability than entrusting oversight to a different agency.

Research Design Criteria

What biometric technologies, ideally used in tandem, best suit the goal of maintaining state and human security without sacrificing either? This broad query can be broken down into three major questions: What techniques are most reliable? What techniques are most unobtrusive? Finally, what techniques are most feasible, both economically and politically? Firstly, reliability hinges first on a fairly important question that is sometimes overlooked in discussing biometric identification systems—which technologies are well-enough developed to be implemented in the immediate future, and could the requisite data be compiled? There are plenty of examples of fingerprint, iris, or retina scan systems set up around the world, but the implementation of more exotic forms from facial recognition to gait analysis seem perpetually in the theoretical stage. After analyzing which technologies are actually available for potential implementation, it is important to ascertain the false positive and false negative rates of such devices. While accepting official reliability statistics on the face value of the corporations or governments who develop them may be problematic, it still serves as a useful first step—private tests by privacy or civil liberties organizations should be viewed with similar suspicion, as they too have an agenda to promote. If designing an overlapping system for example, according to Jain, Ross, and Pankanti, the ideal combination would be fingerprint, face, and iris—each has particularly great strengths, and the likelihood of even one false positive or negative aligning with a second is minimal (Jain, Ross, and Pankanti: 127). But privacy advocates will always counter that, even if something like iris scan technology reduces the chance that any two people would be identical to the test to 1 in 10^{78}, there is no guarantee that the computer's record of whose iris goes with who has not been tampered with (Garfinkel: 56), not to mention that privacy advocates feel statists should themselves be concerned about the ability of facial recognition systems to "out" undercover agents, diplomats, and other government officials who rely on anonymity (Ibidem: 57)—though presumably statists would say that this very aspect of data insecurity could allow governments to circumvent their own systems … but would that be a wise argument to make?

Also troublesome for this selection phase is the issue of actually obtaining the data required to operate advanced biometric identification systems. Though scattershot data like fingerprints and photographs are available from extant occupational requirements, identity documents, and other societal identity implementations, it seems most likely that those individuals whose identification is most sought will be those least likely to have the requisite information available to authorities—though as far as terrorism is concerned, the statist would point out that prior to the World Trade Center attacks, nearly ¾ of terrorist attacks on American soil in two decades were thought to be the work of domestic individuals whose identities would likely be known (Watson: 1). That said, increased global cooperation to solve the problems of terrorism and transnational crime, in conjunction with large-scale identification efforts like India's goal of giving every citizen an identity card within three years (Bajaj: 1), could start to make real inroads in this

avenue—today's terrorists would likely try to avoid identification, but tomorrow's would be unlikely to think that far ahead, and many biometrics, particularly fingerprints and iris prints, stay the same over the lifespan of an individual (Jain, Ross, and Pankanti: 127). However feasible India's plan to hand out over a billion identity documents in three years may be, it is still telling that technology and government centralization have reached the point where such actions are being seriously undertaken, particularly by the second most-populous country in the world.

Reliability's importance to state security and human security are similar and important: neither of these can be properly protected without a trustworthy system overseeing identity checkpoints. State security hinges even more dramatically on reliability than does human security in a sense, as the costs of false negatives (the worst-case state security scenario) are much greater than false positives (the worst-case human security scenario, though the damage potentially caused to individual lives by false negatives should not be overlooked either). Reliability will ultimately help persuade governments to adopt biometric technologies and help persuade publics to be less fearful of biometric technologies. There are many different ways to view the reliability of a particular system; the universality, distinctiveness, permanence, and collectability of identifiers, and the performance (speed and cost), societal acceptability, and resistance to circumvention of systems are all important to reliability considerations (Jain, Ross, Pankanti: 127). As discussed earlier, no single system scores "high" in all categories and thus would be appropriate for all situations, though a combination of face and iris scans or face and fingerprint scans would overall achieve such a rating in each category (Ibidem: 127).

Unobtrusiveness, as mentioned in passing with the earlier example of Las Vegas casino security, is a more difficult concept to measure. Certainly, a system that scans the hand contours of unaware passers-by (Malassiotis et alia: 12) is more unobtrusive than the traditional fingerprint swipe system used in many current biometric implementations. However, it is also important not to sacrifice too much reliability for unobtrusiveness, lest the purpose of the identification systems be defeated. One interesting potential avenue for increasing unobtrusiveness lies in research into so-called adversarial surveillance systems, where devices are specifically designed with the assumption that their targets are actively trying to avoid detection and they must succeed in their surveillance mission regardless (Singh & Kankanhalli: 552). If, as in this example, two researchers working on a project in their spare time can create a system that succeeds up to 80% of the time in capturing high-definition photographs of subjects actively trying to dodge and weave their way out of the view of cameras (Ibidem: 561), it is easy to imagine that checkpoint-based biometric technology utilizing such excellent cameras could succeed in obtaining similarly high-quality photographs of their likely less-antagonistic subjects, eliminating the need for systems like the vaguely menacing Portuguese glass boxes discussed earlier.

Feasibility is a partially quantitative-friendly measurement: economic feasibility can be measured partly through the raw cost of producing and distributing the technologies in question. These costs, however, are themselves somewhat misleading, as implementation costs are not nearly as straightforward, and can mean that initial roll-out costs for identification systems end up wildly missing the mark (BBC [2]: 1, ACLU: 1). Biometric identification is also not the first thing that likely comes to mind when shooting for a goal of cheap but reliable protection; indeed, such systems were notably absent from O'Hanlon et alia's list of cost-effective security techniques (O'Hanlon et alia: 4), though they do note that overall, significant spending beyond the already significant amount allotted by the government for security will be required (Ibidem: 9). Furthermore, there is the problem of political feasibility, something that has particularly bedeviled many such projects, including but not limited to the over-budget identification system roll-outs mentioned above. One suggested way to help smooth over the enormous costs to the government and make new programs more politically palatable is to have private sector organizations pick up part of the cost for their own protection whenever possible (O'Hanlon et alia: 10), though this would likely come with its own share of security concerns.

Research Design

This analysis seeks to lay out the idea that the implementation of biometric identification systems has lead, and will continue to lead, to a future where individuals have a harder time hiding in "plain sight." As suggested earlier in the linkage of American biometric identification checkpoints with Indian national identification databases (which presumably will lead to Indian adoption of biometric checkpoints to put their new cards to use), biometric

identification system proliferation should lead to further biometric identification system proliferation in the modern terrorist climate in a similar spiral to the Cold War proliferation of surveillance technology (Smith: 97-99), which in turn will lead to a greater amount of data available for use in biometric identification. The nature of the research requires a descriptive longitudinal research design using case studies, with hypotheses examining the impact of instituting biometric identification systems in different airports around the world.

Hypotheses

(H1) As increasing numbers of states implement biometric identification systems, the overall effectiveness of the systems will increase. "Effectiveness" is defined here as the number of successful identifications of persons of interest to governments. This is due to the increasing amounts of data available for analysis and sharing with other countries' systems (and the assumption that countries will find it increasingly beneficial to share their information [related to United Nations Resolution 1373]—a separate hypothesis, perhaps, but not one analyzed here). System interoperability issues will likely complicate the relationship, and this hypothesis makes no claim that this "effectiveness" will be free from governmental abuse—but this leads to the second hypothesis. As the first hypothesis represents state security interests, a parallel hypothesis recognizing human security concerns is important to postulate: (H2) as increasing numbers of states implement biometric identification systems, the overall number of complaints due to false positives will drop. Why should this drop, rather than raise? Because whatever potential biometric identification possesses for exploitation or blackmail, its function for identification seems superior to human checks alone. The third and final narrower hypothesis is that (H3) the number of complaints regarding targeted harassment should fall to near-zero following the implementation of biometric identification. Taking the human element of selecting suspicious-looking individuals out of security checks should have the side effect of creating an overall less threatening security environment.

Case Selection and Data Collection

These hypotheses will be applied to cases selected from airports with well-established biometric identification systems: Schiphol Airport in Amsterdam, Heathrow Airport in London, and Los Angeles International Airport. For the first hypothesis, it will then be necessary to obtain government sources for the number of wanted persons detained at these specific crossings, both for periods before and after the biometric identification systems went into use. If the country does not release such statistics, a proximate measure by a non-governmental organization or media source will be sought. If such detail is simply not forthcoming, then it may be necessary to replace the airport with another. Overall, if the hypothesis is correct, there should be statistically significant positive correlation in the effectiveness of such systems identifying persons of interest with the number of countries using such systems.

For the second hypothesis, it is important to obtain potentially more tightly-guarded information, as governments are unlikely to seek publication of false positive complaints. But such sources will still be sought from governments, and barring official government sources the material will again be sought from non-governmental organization or general media sources, again excluding the country from the analysis if no information can be found. Overall, if the hypothesis is correct, there should be a statistically significant negative correlation between the number of complaints in a given country regarding false positive border stops and the number of countries using biometric identification systems. The logic here ultimately comes back to Ted Kennedy: the suspected terrorist who occasionally used the "T. Kennedy" (though if Edward Kennedy had used his real name on his boarding pass maybe this could have been avoided) would be less able to have his identity remain so vague if his fingerprints or face existed in a database—and similarly, as privacy advocates point out, if the FBI made any effort to actually implement the transparency it claimed would exist in the watch list (Hulnick: 207), problems might decrease.

For the third hypothesis, the information may be still harder to obtain than the general number of complaints regarding false positives. The information will still be sought in the same way as the first two, and if the hypothesis is correct, then there should be a statistically significant negative correlation between the implementation of biometric identification systems at an airport and the number of complaints about racial or ethnically-profiled targeting. There seems to be every reason to expect this outcome, given that a major purpose of such technology is to remove human bias from identification.

Other Factors

It is likely that these hypotheses will be complicated by the degree to which biometric identification is implemented at the airport. If Heathrow and Schiphol expand their fingerprinting and iris scans while Los Angeles International holds back, then it is certainly likely that data for the first two hypotheses will reflect this lesser implementation through a lesser impact. The third hypothesis, however, should be resilient against this, as implementing any form of biometric identification should help fight discrimination—though if the systems are for optional convenience instead of universal, then their impact will be limited. To control for this in the analysis, each type of biometric identifier used at each airport will be recorded separately, so that it can be quickly seen or calculated as to whether the number or type of different biometric identification technologies has an impact on the success of the hypotheses. It is also important to record whether each airport currently uses biometrics for the general populace of the airport or as an elite pass system—the latter would render the airport useless for the first hypothesis, though the others could still be tested.

Conclusion

To the communitarian, the question of surveillance versus privacy is a struggle between confidence and fear (Brin: 314). To the privacy advocate, surveillance versus privacy is a struggle between tyranny and freedom (Rosen: 60). To the statist, surveillance versus privacy is a struggle between providing security and not providing security (Lloyd: 257-258). Which perspective is correct merely depends on individual interests and goals—just as “Every Breath You Take” can be heard either as a menacing song about stalking or a soothing song about a loving caretaker (Marx: 200), biometric identification represents both the good and the bad of surveillance. Biometric identification systems are both a very real possibility and a very real problem thanks to the the ever-advancing technology potentials of the modern world, and either implementing all systems wherever they could be implemented due to their assured increased effectiveness, or stopping all systems from being implemented due to privacy and civil liberties concerns, will be detrimental to state and human security alike due to their very real shared interests as discussed in the introduction. The only way to ensure that safeguards are in place to stop any individual set of concerns from usurping the overall security picture is to seek a relatively objective understanding of which technologies are most reliable, which are most unobtrusive, and which are most economically and politically feasible for implementation. New technologies are seemingly developed on a regular basis, and governments and corporations alike might imagine that upgrading to a new system that is objectively superior to the old system in every way is desirable—but the cost in collecting the new information required for the new system may make any new progression a logistical nightmare. It is better to have a full picture of all extant technologies and all on-the-horizon technologies before committing to any sort of wide-scale implementation of biometric identification systems, but of course asking political progress to come to a halt while scientists work out the details does not sound like a recipe for success—all the more problematic to privacy advocates as “each new method and each new reason for identifying people—has been just tacked onto past practice, unconsidered. This is the policy-development equivalent of auto repair by electrical tape and baling wire” (Harper: 2).

In a sense, surveillance technologies can be inherently constructed in one of two ways, either to facilitate transparency in operation, or to facilitate spying (Garfinkel: 259). Counterintuitively, systems designed to be covert may actually be more beneficial to overall human security transparency concerns, thanks to downplaying the overall obviousness and intrusion of surveillance systems. Cameras are bound to continue shrinking in size and growing in ability for the indefinite future—thus, not only might it be a lost cause to strive for surveillance systems to be transparent in and of themselves, it might be far more effective to seek political transparency rather than technological transparency, that is to say seeking open and accountable false-positive appeal procedures rather than clearly labelling the location and function of every surveillance device. Stopping the spread of surveillance into wider society represents a challenge, but the balance of state and human security requires that definite limits to such technologies exist lest the system be thrown out entirely (Scott, Tehranian, and Mathias: 48)—or, alternately, as Brin suggests, that such surveillance systems become open to access by the public as well as by the government, thus creating a world in which surveillance is universal (Brin: 14).

BIBLIOGRAPHY

American Civil Liberties Union (ACLU). 2008. "Fuzzy Math and the Real Cost of Real ID." *ACLU National Security*. Accessed on November 8, 2009, from http://www.aclu.org/national-security/fuzzy-math-and-real-cost-real-id

American Civil Liberties Union (ACLU) [2]. 2006. "TSA and FBI Ordered to Pay $200,000 to Settle 'No Fly' Lawsuit." January 24. Accessed on November 9, 2009, from http://www.aclu.org/national-security/tsa-and-fbi-ordered-pay-200000-settle-no-fly- lawsuit

American National Standards Institute (ANSI). 2005. "Machine Readable Passports to be Standard Worldwide by 2010; ICAO symposium offered to support implementation." *ANSI News & Publications*. August 10. Accessed on November 8, 2009, from http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=1011

Arena, Kelli, & Cratty, Carol. "FBI wants palm prints, eye scans, tattoo mapping." *Central News Network*. February 4, 2008. Accessed on November 5, 2009, from http://www.cnn.com/2008/TECH/02/04/fbi.biometrics/

Bajaj, Vikas. 2009. "India Undertakes Ambitious ID Card Plan." *New York Times*. June 25. Accessed on December 4, 2009, from http://www.nytimes.com/2009/06/26/world/asia/26india.html

Baldor, Lolita C. "Military seeks better use of finger, eye scans: U.S. bases just 20 miles part (sic) have different identification requirements." *MSNBC*. January 28, 2009. Accessed on November 7, 2009, from http://www.msnbc.msn.com/id/28893152/

Bogatin, Donna. "Walt Disney World 'fingerprinting' visitors: Magic Kingdom, or Mickey Mouse?" ZDNet. September 4, 2006. Accessed from http://blogs.zdnet.com/micro- markets/?p=411 on November 8, 2009.

Brin, David. 1998. *The Transparent Society*. Reading, Massachusetts: Addison-Wesley.

British Broadcasting Corporation (BBC). "Pet Shop Boys protest at ID cards." *British Broadcasting Corporation*. March 1, 2006. Accessed on November 5, 2009, from http://news.bbc.co.uk/2/hi/uk_news/politics/4763874.stm

British Broadcasting Corporation (BBC). [2] "Whitehall Fights ID Cost Demand." BBC News. July 5. Accessed on November 7, 2009, from http://news.bbc.co.uk/1/hi/uk_politics/5150584.stm

Cook, Blanche Wiesen. 1978. "Surveillance and Mind Control" in *Uncloaking the CIA*. Howard Frazier, editor. 174-189. New York: Collier Macmillan Publishers.

Etzioni, Amitai. 1999. *The Limits of Privacy*. New York: Basic Books.

Federal Bureau of Investigation (FBI). 2008. "FBI Announces Contract Award for Next Generation Identification System." February 12. Accessed on November 9, 2009, from http://www.fbi.gov/pressrel/pressrel08/ngicontract021208.htm

Ferro, Marcello, Giovanni Pioggia, Alessandro Tognetti, Nicola Carbonaro, and Danilo De Rossi. "A Sensing Seat for Human Authentication." IEEE Transactions on Information Forensics and Security, Volume 4, Number 3 (September, 2009). Pages 451-459.

Garfinkel, Simson. 2000. *Database Nation: The Death of Privacy in the 21st Century.* Cambridge, England: O'Reilly.

Goo, Sara Kehaulani. 2004. "Sen. Kennedy Flagged by No-Fly List." *Washington Post*. August 20. Accessed on December 4, 2009, from http://www.washingtonpost.com/wp-dyn/articles/A17073-2004Aug19.html

Gotlieb, Calvin C. 2003. "Privacy: A Concept Whose Time Has Come and Gone" in *Computers, Surveillance, and*

Privacy. Minneapolis: University of Minnesota Press. 158-169.

Graziano, Claudia. 2003. "Learning to Live With Biometrics." *Wired*. September 9. Accessed on November 8, 2009, from http://www.wired.com/politics/security/news/2003/09/60342

Harper, Jim. 2006. *Identity Crisis: How Identification is Overused and Misunderstood*. Washington, D.C.: Cato Institute.

Harris, Dan. 2002. "Call for Tighter Security Comes at a Cost." *ABC News*. July 5. Accessed on November 9, 2009, from http://abcnews.go.com/WNT/story? id=130263&page=1&page=1

Hesseldahl, Arik. 2005 "One-Fingered Discount At The Grocery Store." *Forbes*. June 17. Accessed on November 8, 2009, from http://www.forbes.com/2005/06/17/digital-life-fingerprint-scanners-cx_ah_0617diglife.html

Honan, Edith. 2007. "Bloomberg defends city surveillance camera plan." *Reuters*. October 2. Accessed on November 7, 2009, from http://www.reuters.com/article/politicsNews/idUSN0243142020071002

Hulnick, Arthur S. 2004 *Keeping Us Safe: Secret Intelligence and Homeland Security*. Westport, Connecticut: Praeger Publishing.

Jain, Anil K., Ross, Arun, and Pankanti, Sharath. 2006. "Biometrics: A Tool for Information Security." *IEEE Transactions on Information Forensics and Security*, Volume 1, Number 2 (June). Pages 125-143.

Liptak, Adam. 2008. "1 in 100 Adults Behind Bars, New Study Says." *The New York Times*. February 28. Accessed November 6, 2009, from http://www.nytimes.com/2008/02/28/us/28cnd-prison.html

Lloyd, Martin. 2003. *The Passport: The History of Man's Most Travelled Document*. Thrupp, Stroud, United Kingdom: Sutton Publishing.

MacFarlane, S. Neil, & Khong, Yuen Foong. 2006. *Human Security and the UN: A Critical History*. Indianapolis: Indiana University Press.

Marx, Gary T. 2003. "Electric Eye in the Sky: Some Reflections on the New Surveillance and Popular Culture" in *Computers, Surveillance, and Privacy.* Minneapolis: University of Minnesota Press. 197-200.

O'Hanlon, Michael E., Peter R. Orszag, Ivo H. Daalder, I. M. "Mac" Destler, David L. Gunter, Robert E. Litan, & James B. Steinberg. *Protecting the American Homeland: A Preliminary Analysis*. Harrisonburg, Virginia: R. R. Donnelley and Sons.

Peterson, Scott. "Under fire, US marines hand off battered Fallujah." *The Christian Science Monitor*. November 24, 2006. Accessed on November 8, 2009, from http://www.csmonitor.com/2006/1124/p01s04-woiq.html

Polowczuk, Susan. "Clemson facial recognition research advances." *Clemson University Newsroom*. Accessed on November 3, 2009, from http://www.clemson.edu/media-relations/article.php?article_id=2137

Malassiotis, Sotiris, Aifanti, Niki, & Michael G. Strintzis. 2006. "Personal Authentication Using 3-D Finger Geometry." *IEEE Transactions on Information Forensics and Security*, Volume 1, Number 1 (March). Pages 12-21.

Martin, Guy. 2007. "Will This City Save Us All?" *Condé Nast Publications*, February. Pages 112-117, 150, 153-154.

NEC. "Biometrics identification technology (Singapore)." 2007. NEC Biometrics Security Solution. Accessed on

November 8, 2009, from http://www.nec.com/global/onlinetv/en/society/e_pass_l.html

Parenti, Christian. 2004. *The Soft Cage*. Jackson, Tennessee: Basic Books.

Paris, Roland. "Human Security: Paradigm Shift or Hot Air?" 2001. *International Security*, Volume 26, Number 2 (Autumn), pages 87-102.

Scott, James C., John Tehranian, and Jeremy Mathias. 2004. "Government Surnames and Legal Identities" in *National Identification Systems: Essays in Opposition*, Carl Watner and Wendy McElroy, editors. 11-54. Jefferson, North Carolina:McFarland & Company.

Singh, Vivek K., & Kankanhalli, Mohan S. 2009. "Adversary Aware Surveillance Systems." *IEEE Transactions on Information Forensics and Security*, Volume 4, Number 3 (September). Pages 552-563.

Smart Airlock Control System (SMACS). 2006. "For Biometrics – the Future Has Just Begun." *Product Info*. Accessed from http://www.smacs.com/index.php?option=com_content&task=view&id=18&Itemid=1 on November 8, 2009.

Smith, Robert Ellis. 2000. *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Providence: Sheridan Books.

Thomas, Kim. 2009. "School puts a brave face on biometrics." *The Guardian*. March 5. Accessed on November 8, 2009, from http://www.guardian.co.uk/technology/2009/mar/05/biometrics-data-protection

Travis, Alan. 2009. "Lords: rise of CCTV is threat to freedom." *The Guardian*. February 6. Accessed on November 9, 2009, from http://www.guardian.co.uk/uk/2009/feb/06/surveillance-freedom-peers

United Kingdom Home Office Border Agency, (UKHOBA) *Iris Recognition Immigration System (IRIS)*. Accessed from http://www.ukba.homeoffice.gov.uk/managingborders/technology/iris/ on November 7, 2009.

United Nations Development Project, *Human Development Report 1994*. 1994. Accessed from http://hdr.undp.org/en/reports/global/hdr1994/ on November 7, 2009. New York.

Wang, Tova Andrea. 2002. "Issue in Brief: The Debate Over a National Identification Card." May 10. *The Century Foundation Homeland Security Project*. Accessed on November 7, 2009, from www.tcf.org/Publications/HomelandSecurity/National_ID_Card.pdf

Watner, Carl. 2004. "Drivers Licenses and Vehicle Registration in Historical Perspective" in *National Identification Systems: Essays in Opposition*, Carl Watner and Wendy McElroy, editors. 103-116. Jefferson, North Carolina: McFarland & Company.

Watner, Carl, and McElroy, Wendy. 2004. "Introduction" in *National Identification Systems: Essays in Opposition*, Carl Watner and Wendy McElroy, editors. 1-9. Jefferson, North Carolina: McFarland & Company

Watson, Dale L. 2002. "The Terrorist Threat Confronting the United States," Testimony before the Senate Select Committee on Intelligence. February 6. Washington, D.C. Accessed on November 29, 2009, from www.fbi.gov/congress/congress02/watson020602.htm

[1] The terminology of "human security" is actually rarely, if ever, used by those defending its principles, perhaps due in no small part to the particularly vague nature of the term (Paris: 88), but it is important to acknowledge the similarity of the general concerns about biometric identification the outlines of this concept.

[2] Though there seems to be no research on whether biometric identification can separate identical twins.

—

Written by: Andrew M. J. Huntleigh
Written at: University of Delaware
Written for: Dr. Stuart Kaufman
Date written: Fall 2010