3

Finding the Face of Terror in Data

> During the Cold War, the enemy was predictable, identifiable, and consistent. We knew the threats, the targets were clear. But times change. Today, with the demise of the other superpower, America is in a different position: a position of vulnerability. When the enemy strikes, it isn't predictable. It isn't identifiable. It is anything but consistent. Times change. We are in a world of "asymmetrics," and we need transformational solutions. The asymmetric threat is now a reality of global life. How do we detect it? How do we predict it? How do we prevent it?
>
> —Promotional video for the Total Information Awareness program, 2002

> In a top ten list for 2000, the next nine countries' defense budgets do not *add up* to the United States's. As remarkable as the sheer size of the military budget might be, it begs a larger question, which in the rush to reach a budget agreement went mostly undebated: just where is this enemy who justifies such expenditure?
>
> —James Der Derian, *Virtuous War*

From the Cold War to the War on Terror

In his keynote address at the September 2002 Biometrics Consortium Conference, Dr. Robert L. Popp, then deputy director of DARPA's newly formed Information Awareness Office, began by showing a promotional video for the "Total Information Awareness" (TIA) program. TIA would later spark public controversy and bipartisan political opposition, but the press had not yet taken notice of it, and the conference audience of industry and government officials seemed interested and receptive. The video, outlining the various research and development projects combined to form TIA, opened with

a montage of images and sounds signifying the Cold War, the fall of the Berlin Wall, and the newly defined U.S. security threats of the 1990s and early twenty-first century. The Cold War images—black and white photos of suffering peasants and video of Soviet soldiers marching in file—were followed by mug shot images of recognizable terrorist suspects, including Osama bin Laden, and a familiar video image of a crowd of Arab men moving rhythmically en masse. This visual montage accompanied the voice-over narration quoted above proclaiming "the asymmetric threat" as "now a reality of global life."

Providing a simple narrative of transition from the Cold War to the "war on terror," the video contrasted these new "asymmetric threats" with the more symmetrical geopolitical conditions that existed prior to the breakup of the Soviet Union. The text invoked a nostalgic longing for the predictability and consistency of the Cold War, when the enemy was ostensibly well-defined and *identifiable*, combining it with an almost gleeful futurism about the promise of new digital technologies to save the West from its uncivilized Other. The idea of an "unidentifiable" enemy presented a new form of national vulnerability—"America" was now "vulnerable" precisely because it could not identify its enemy. The United States seemed more in danger than ever, with the "asymmetric threats" facing the nation in the post–Cold War context even greater than the perpetual threat of nuclear holocaust during the arms race with the Soviet Union. The collapse of the communist regimes may have dissolved the symmetric threat of nuclear warfare with the "other superpower," but in its place came many other villains more difficult to locate, define, and identify.

Although it is not difficult to discern problems with the suggestion that nation's Cold War enemies were easily identifiable, the fall of communism did in fact create new security risks for the United States, destroying the balance of global power that had created a relatively stable international order in the four decades following World War II.[1] In addition to specific new threats, the demise of the "other superpower" presented another sort of vulnerability for the U.S. national security state: a crisis of legitimacy. In the 1990s, a rising volume of criticism questioned why the United States was still spending ten times as much on defense as its closest defense-spending competitor, and nearly as much as the rest of the world combined. Just where was the enemy that justified this expenditure? As one response to this question, military strategists placed special emphasis on "asymmetric threats," a trope that not only embodied a questionable claim to the unique nature of the new post–Cold War adversaries, but also invested relatively small threats with

greater threat potential, aiming to provide some justification for the ongoing reproduction of the imperial-sized, Cold War national security apparatus. The United States may no longer have an enemy that could match its military might, according to this message, but it now has more insidious enemies that do not play by the conventional rules of state warfare, and thus represent significant threats to the nation, disproportionate to their relatively minuscule military resources.

The military discourse that defined these new "unidentifiable" and "inconsistent" enemies as major security threats was given considerable leverage by the enormity of violence on 9/11 along with its precession as simulacra. The TIA promotional video exemplified the way that state security discourse constructed both the threat of terrorism and the appropriate security strategies to address that threat in the aftermath of the catastrophe. The ambiguous signifier of asymmetric threats became a chosen mantra of state security discourse, an allegedly new type of danger that required considerable research and investment into new types of war-fighting technologies. The tropes of "asymmetric threats" and "unidentifiable enemies" provided justification for a set of policy proposals after 9/11, including arguments in favor of stepped-up funding for the development and widespread deployment of facial recognition and other biometric identification systems. Given the problem of small but highly dangerous enemies that were increasingly difficult to identify, the need to develop and deploy expensive, new, high-tech surveillance technologies at a proliferation of sites seemed self-evident.

There were of course other forces at work shaping the political response to 9/11. As we saw in chapter 1, the political-economic priorities of neoliberalism had a major influence on the demand for network security technologies in the 1980s and 1990s, including facial recognition and other biometrics, and these priorities played a significant role in defining the political response to the attacks. It was immediately apparent that the events of 9/11 would be a major boon to providers of security systems and services, an industry deeply connected to the information technology sector. As the enthusiastic response of both security and IT brokers clearly evidenced, post-9/11 security provision would involve ventures aimed at maximum profitability, and the business of security would overlap considerably with the business of information technology. In fact, long before 9/11, the information and security sectors were so tightly integrated as to be virtually inseparable; the major players in the IT sector were hard at work developing network security systems, and both state and private-sector entities conventionally understood as security providers had long since integrated IT into all manner of security

systems. Thus it was unsurprising to find an industry observer from *Intelligent Enterprise* noting with optimism that "homeland security spending will help fuel an IT recovery. IT solution providers may some day look back on the War on Terror and be grateful for the opportunities born out of turmoil."[2] Such pronouncements not only articulated the overlapping dimensions and priorities of security and IT, they also offered a clear expression of the market logic that would define what "homeland security" and the "war on terror" meant in practice.

Proponents of biometrics in particular saw a major opportunity to capitalize on the emerging "homeland security" regime, and in fact to participate in the very construction of the strategies and programs that would define what homeland security looked like in practice. The 9/11 attacks happened at a time when vendors of facial recognition systems were beginning to experiment with real-world applications, from Department of Motor Vehicle offices in the United States, to voter registration systems in Mexico and other countries, to Smart CCTV experiments in London and Tampa. As we saw in chapter 1, the application of biometrics for the "securitization of identity" was already taking place to satisfy industry demand for priorities like network security, labor control, and consumer tracking. State agencies likewise had already begun adopting biometrics as part of the more repressive apparatuses of the penal-welfare-immigration-control complex. In the language of cultural studies, the aftermath of 9/11 was a moment of articulation, where objects or events that have no necessary connection come together and a new discursive formation is established: automated facial recognition as a homeland security technology, a means of automatically identifying the faces of "terrorists." The interests of biometrics industry brokers to push their technologies after 9/11 translated well into the prevailing public policy and press response to the attacks: the frenzied turn to "security experts" to speculate as to the source of security failures and to provide recommendations for "stopping the next one."[3]

The biometrics industry readily answered the call for expert knowledge of security issues and technologies, positing their identification systems as *the* solution to the new terrorist threat. The spokespeople for the biometrics industry worked feverishly to promote biometrics as central components in new security systems and to situate themselves and their companies as "moral entrepreneurs" taking charge in a moment of national crisis. Industry brokers issued press releases, appeared in the press on a regular basis, and testified before Congress as to the benefits of their products. Most impudent, proponents of facial recognition technology repeatedly suggested that such systems could have prevented at least one if not all of the hijackings.

While military needs influenced the development of automated facial recognition since its inception as a research program, the technology took on special importance in state security discourse after 9/11, as advocates took the opportunity to catapult it from set of technological experiments into something more closely resembling what Bruno Latour calls a "black box"—a functioning technology positioned as virtually indispensable to a secure, technological future.[4] Facial recognition technology would ostensibly provide an accurate, objective, precision-guided means of identifying the faces of terrorists as they attempted to pass through airport security, border control stations, and a proliferation of other checkpoints. The technology promised to succeed where human security staffers failed, compensating for their imperfect, subjective perceptual abilities and limited memory capacities.

This chapter examines the preoccupation with facial recognition technology in the post-9/11 context, unpacking claims to its technical neutrality by investigating the cultural logic that defined the technology and the practical politics that shaped system development. While the promise of facial recognition lay in its potential to individualize the terrorist threat by targeting specifically identified "terrorist" individuals, the effort to define it as a homeland security technology also made use of an implicit classifying logic, including rhetorical moves that resuscitated antiquated notions of deviant facial types. In practice, facial recognition technology seemed uniquely suited to identifying the individual faces of "terrorists." But in a more symbolic sense, the technology promised to provide a means of "protecting civilization" from a more generalized and racialized "face of terror." Although facial recognition algorithms were not expressly designed to classify faces according to racial typologies, the symbolic authority of the technology in the post-9/11 context very much depended on the idea that it could in fact be used to identify a mythic class of demonic faces that had penetrated the national territory and the national imagination. The "facialization" of terrorism—defining nonstate forms of political violence with recourse to the racist logic of a mythic, demonized facial type—was prevalent in discourse about facial recognition technology, appearing alongside claims about its technical neutrality.

If claims to the technical neutrality of automated facial recognition disavowed the meanings assigned to it, they also denied the forms of social differentiation it promised to accomplish, offering too narrow a view of how surveillance and identification systems function. The application of automated facial recognition for "terrorist" identification required more than the development of algorithms for digitizing the face or the deployment of biometric capture devices. It also required the construction of a terrorist classifi-

cation system—a technology for *making up terrorists*—that took the tangible form of a consolidated watchlist database. Like the central role of the archive in the application of photography to criminal identification, the database is at the heart of biometric system development. In order to understand how facial recognition systems function, it is crucial to have some sense of how facial image databases are constructed, especially the social forces governing their form and content. How are facial image databases populated? What identities are entered into a database and why? What information about them is archived? How is that information organized, and how is the "accuracy" of the information determined? As noted in the previous chapter, these are policy questions, as well as questions about the practical design of identification systems. But they are also questions about the meaning of facial recognition technology, and about the politics that inform system development. A close look at terrorist watchlist database consolidation demonstrates the way that classification systems, enshrined in the material form of the database, construct rather than merely reflect the identities they purportedly represent. It also shows that, in practice, there is nothing neutral about the way computers are being programmed to "see" the face.[5]

Racializing the Terrorist Threat

On the eve of the second anniversary of 9/11, the *New York Times* published an op-ed piece by John Poindexter, the former national security adviser to Ronald Reagan best known for his involvement in the Iran-Contra scandal. Poindexter had recently been appointed as head of the Total Information Awareness program, a set of funding initiatives for research and development into new data mining and analysis technologies that would make optimal use of the full range of available public- and private-sector databases to gain knowledge about the identities and activities of "terrorists." Although all the research programs gathered together under TIA existed in some form before its creation, in its newly organized form it received widespread criticism as having an overly Orwellian mission to spy on Americans. As a result of bipartisan opposition to TIA, Congress moved to defund the program in the summer of 2003. Poindexter's op-ed piece in the *Times* was an effort to defend TIA's parent agency, DARPA, from further funding cuts, arguing for the importance of DARPA's research programs and the agency's neutrality with respect to any applications that resulted from the research it funded.

If Poindexter's appeal itself was important for what it revealed about the politics of military R & D in the post-9/11 context, it was less compelling than

the headline of the article and the image it conjured: "Finding the Face of Terror in Data."[6] Referencing sophisticated new techniques of data mining, the headline also carried with it powerful connotations of national contamination, along with the implication that new digital technologies could be used to purify the nation of its enemies within. Computerized forms of data analysis and retrieval were continuously held out in the wake of 9/11 as a means of identifying hidden information vital to uncovering terrorist plots. The idea that Poindexter or DARPA or anyone else could "find the face of terror in data" implied that there actually existed a "face of terror," a particular type of face characteristic of terrorists, and that large data sets could be mined in search of relationships and patterns that would reveal their identities. In other words, in the process of infiltrating civilized society, "terrorists" have left traces of their presence in the parallel world of data, society's digital mirror image. Like Trojan horse computer viruses, they would need to be identified, isolated, and eradicated using the most sophisticated forms of data mining and analysis. The technological projects cobbled together under DARPA's TIA program each claimed to provide a technical means of national purification, a sophisticated, high-tech approach to targeting external and internal threats to the population so that the nation could remain healthy and vibrant in the face of newly recognized hazards and contaminants.

Neither Poindexter's headline nor the article itself made explicit claims about facial recognition technology specifically, but it required no stretch of the imagination to see it there, as one among an array of technical means that would ostensibly help authorities locate the "face of terror" in the field of data circulating over global IT networks. In fact, one of the programs placed under the TIA umbrella during the program's brief tenure was the "Human ID at a Distance" initiative, or Human ID for short, a DARPA program formed after the bombing of the Khobar Towers U.S. military barracks in Saudi Arabia in 1996. Originally called "Image Understanding Force Protection," Human ID provided funding to university research labs and private companies doing research on biometric technologies, with the ultimate aim of developing and fusing multiple biometrics (face, voice, gait) into one, more robust automated sensory system that could identify individuals from a distance, such as around the perimeter of U.S. military installations. The goal was to develop image analysis technologies that could be applied to improve on military surveillance systems and protect U.S. military forces abroad, especially in the Middle East.

DARPA's Human ID biometrics funding initiative was part of a broader U.S. military strategy, no less than a "revolution in military affairs" aimed at

developing command, control, and communications technologies in order to achieve "global information dominance."[7] The history shared by computer science and engineering on the one hand, and military research and development on the other, has been well documented.[8] The drive to develop autonomous weapons systems in particular has been at the center of artificial intelligence research since its inception, including the effort to invest computers with synthetic forms of perception (vision and hearing).[9] Although the military has never fully handed decision-making authority over to computers, military applications of AI have increasingly blurred the distinction between merely "advisory" and fully "executive" capabilities.[10] The development of imaging technologies that could automatically identify targets "at a distance" has been a part of this effort to create new and more effective human-computer war-fighting assemblages, with a certain level of authority and perceptual capacity translated into automated systems. Fueled by a strategy of "global vision," military R & D has aimed to integrate new visualizing technologies and weapons systems in order to form what Paul Virilio has called a "logistics of military perception," whereby the major global powers dominate using technologies for attending perpetually and immediately to images and data, keeping targets constantly in sight.[11] Under these conditions, according to Virilio, the perspective of "real time" supersedes the perspective of "real space" (invented by the Italians in the fifteenth century), and seeing over distance becomes virtually synonymous with contact—and killing—over distance. The war-fighting promise of automated facial recognition and related technologies lay precisely in their potential to identify objects automatically and "at a distance," whether the final aim was to control, capture, or destroy these targets.[12] In short, in the military context the aim of identification-at-a-distance has been inescapably married to the tactic of killing-at-a-distance.

Political theorists have debated at some length about the paradoxical nature of the modern state's sovereign claim to the right to kill. For Foucault, this problem became especially salient with the emergence of political systems centered on the health and well-being of the population—in other words, with the rise of what he calls "biopower."[13] The historical emergence of this form of political power corresponds to the discovery, along with the formation of the sciences of demography and statistics, of a new object of state intervention in the eighteenth and nineteenth centuries: *the population*. The life of the population itself, as an aggregate of bodies in circulation with one another and with their social and environmental conditions, became an object of intense political and scientific concern. The political technology of biopower became embedded in existing disciplinary techniques that targeted

the individual body, but took a broader view of the individual as a component of a larger collective body, one that had its own qualities and required its own regulatory interventions. Along with the discovery of the population came the corresponding recognition of its variables and vulnerabilities—the forces, such as disease epidemics, draughts, crimes, suicides, and procreative and child-rearing practices, that affected the health of the population. These forces in turn needed to be measured, evaluated, and intervened on in a manner that would make the population as a whole healthier, more secure, and more productive. A whole set of institutions and bodies of knowledge emerged to examine and deal with the health and security of the population, including medicine and public hygiene, insurance, individual and collective savings, safety regimes, and eugenics and antimiscegenation campaigns as well as other formal and informal regulatory controls on sexuality and reproduction.[14] These bodies of knowledge were not strictly repressive but likewise aimed to productively define the range of active, normal, civilized forms of human subjectivity that would be appropriate for modern citizens living in "free" societies.

The question arose, under emerging forms of biopolitical governance, as to how such political systems concerned centrally with the health, well-being, and security of their populations could also claim the sovereign power to kill, "to call for deaths, to demand deaths, to give the order to kill, and to expose not only [their] enemies but [their] own citizens to the risk of death."[15] It is at this point, Foucault argues, that racism intervenes. Racism becomes "a way of introducing a break into the domain of life that is under power's control: the break between what must live and what must die."[16] Racism enables the biopolitical differentiation of the population into categories of relative value in the name of the health and security of the population as a whole. When the security of the total population is paramount, racism becomes the means by which the state claims the legitimate right to kill, and especially to enable its citizens to be killed. To be clear, by "killing" Foucault does not simply mean murder as such, "but also every form of indirect murder: the fact of exposing someone to death, increasing the risk of death for some people, or . . . political death, expulsion, rejection, and so on."[17] The modern state "can scarcely function without becoming involved with racism at some point."[18]

The biopolitics and associated forms of state racism that emerged in the eighteenth and nineteenth centuries are still with us today but continue to evolve and take new forms. "Racism does not . . . move tidily and unchanged through history," writes Paul Gilroy. "It assumes new forms and

articulates new antagonisms in different situations."[19] Likewise, new conditions and instabilities have arisen that challenge the health of populations in large-scale societies, providing impetus for new forms of biopolitical intervention.[20] Many of the global instabilities and crises that the populations of modern nation-states face today are without a doubt what Anthony Giddens calls "manufactured risks"—that is, risks resulting not from natural forces external to human activity, but from human development itself, especially from the progression of science and technology.[21] International terrorism is a paradigmatic example of a "manufactured risk," arguably arising, in the most general analysis, as a result of diverse and even incommensurate cultures coming in contact thanks to imperialistic and expansionist impulses, along with associated developments in communications and transportation systems. Of course, this is not the explanatory picture that is painted of terrorist acts when they occur. Rather, they become acts of sheer and inexplicable evil, and they provide perfect fodder for the intervention of racism into biopolitical forms of government. This was especially salient in the post-9/11 context. As images of Osama bin Laden and the alleged hijackers circulated in the Western media, a powerful metaphoric image of the "enemy Other" took shape. The racialization of the enemy was virtually assured, providing a ready alibi for intensified state investment in the technological infrastructure to support the biopolitical differentiation of the population. Despite the language of "unidentifiable enemies," finding the face of terror in data meant designing and deploying what Lisa Nakamura calls the "socioalgorithmics of race"—new technologies designed to target specific types of faces and bodies (those of Arab men, to be sure, but also all manner of other derelict identities).[22]

The practice of constructing a racialized image of a mythic enemy has long functioned as a way of solidifying and reinforcing national identity.[23] At least since World War II, propagandists have recognized that "the job of turning civilians into soldiers" could be achieved through the uniquely effective tactic of superimposing a variety of dehumanizing faces over the enemy "to allow him to be killed without guilt."[24] The trope of the "face of terror" that circulated widely after 9/11 functioned in this way, offering a caricatured version of "the enemy," while at the same time suggesting the existence of a terrorist facial type. Along with ubiquitous images of the faces of Osama bin Laden and the hijackers—the alleged unidentifiable enemies—the "face of terror" invoked specific objects: mug shots and grainy video images of Arab men. The trope resuscitated a history of creating archetypical racialized enemies, along with the associated practice of "facialization," Karen Engle's term

for the process whereby "the face of a subject, which is believed to reveal an interior truth kernel or deep essence, comes to stand for the narratives a nation tells about itself."[25]

It was not John Poindexter but Visionics Corporation that was the first to make use of the "face of terror" trope. In its initial effort to position itself at the center of the public-private security response to 9/11, the company released a policy "white paper" on September 24, 2001, titled *Protecting Civilization from the Faces of Terror: A Primer on the Role Facial Recognition Technology Can Play in Enhancing Airport Security*. The bold-faced claim that the technology could "protect civilization" can be read as hyperbole only in retrospect; in the immediate aftermath of the attacks it represented a serious statement about the product's capabilities. The "faces of terror" phrase, obviously used as clever means of positioning facial recognition technology as a solution to airport security, also must be understood in the grave climate of the moment. While ostensibly referencing the individual faces of the 9/11 hijackers as well as potential future terrorists, it had more general connotations as well, signifying a metaphoric, racialized enemy Other—a demonic type of face that had penetrated both the national territory and the national imagination.

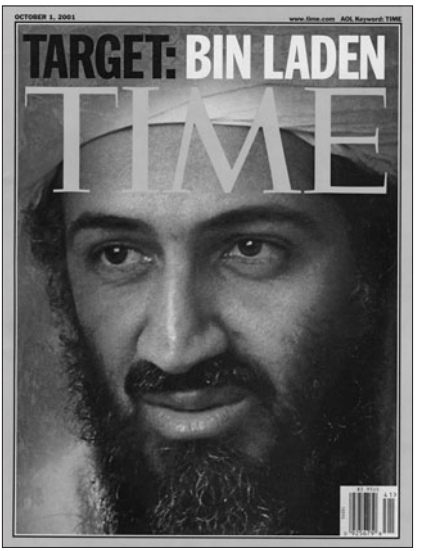
Other uses of the "face of terror" trope in association with facial recognition technology followed. For example, the Technology, Terrorism, and Government Information Subcommittee of the U.S. Senate Judiciary Committee held a hearing on "Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism."[26] Like Visionics' use of the metaphor, such references could be interpreted as merely clever turns of phrase if not for the seriousness of the moment and the extent to which they made unveiled claims about the existence of a terrorist facial type. The "face of terror" trope embodied both an individualizing and a classifying logic of facial representation, sliding from one meaning to another. Interpreted in correct grammatical terms, the phrase referred to individuals with expressions of terror on their faces, but it was used instead in reference to the perpetrators of terrorist acts. The "face of terrorism" would have made more sense but was likely too explicit in its reference to a terrorist facial type. (George W. Bush came closest to using this reference in a statement announcing the FBI's "most wanted terrorists" watchlist: "Terrorism has a face, and today we expose it for the world to see."[27]) In its reference to a representative terrorist face, the trope could not help but resuscitate assumptions from the antiquated science of physiognomy about the existence of relationships between facial features and individuals' essential qualities, including alleged inherent propensities for criminal or other deviant behaviors.

But the image of "the modern face of terror" promulgated after 9/11 did not take precisely the same form as its physiognomic predecessors. Repackaged in digital form and distributed over computer networks, it was more akin to a "virtual enemy"—the simulated adversary of what James Der Derian ironically calls the "virtuous war."[28] This type of war is built on a new war machine, "the military-industrial-media-entertainment network," which merges simulation technologies with lethal weaponry, action movies and video games with civilian and military training exercises, and computer vision with "the logistics of military perception."[29] Specially designed for killing at a distance, this new war machine is no less violent than earlier forms, but claims to use high-tech war-fighting technologies in the service of virtue. When fighting the virtuous war at a distance, it is especially easy to kill the virtual enemy without guilt. And "the more virtuous the intention," writes Der Derian, "the more we must virtualize the enemy, until all that is left as the last man is the criminalized demon."[30] In its metaphoric connection to automated facial recognition, the demonic face of terror functioned like Der Derian's virtual enemy, invoking the image of a digitally generated avatar or morphed composite of "terrorist faces."

The mythic image of a morphed terrorist facial avatar embodied in the post-9/11 "face of terror" trope can also been seen as the antithesis of the now famous computer-generated image of a fictional woman's face printed on the cover of *Time* magazine in the fall of 1993. Deemed the "New Face of America," the image was morphed together from the facial images of seven men and seven women of various ethnic and racial backgrounds, and was used to promote a special issue on "How Immigrants Are Shaping the World's First Multicultural Society." Feminist scholars found the *Time* cover full of familiar and problematic assumptions about race and gender. The notion of race and pure racial types remained deeply embedded in the technique of computer morphology, Evelyn Hammonds argued, and morphing was "at the center of an old debate about miscegenation and citizenship in the United States."[31] The way the fictitious female face conveniently substituted the bodiless practice of morphing for the flesh-and-blood reality of miscegenation similarly made Donna Haraway uncomfortable, particularly to the extent that it effaced a bloody history and promoted a false sense of unity and sameness.[32] According to Laurent Berlant, the "New Face of America" on the *Time* cover was "cast as an imaginary solution to the problems of immigration, multiculturalism, sexuality, gender, and (trans)national identity that haunt the U.S. present tense."[33] The morphed image was feminine, conventionally pretty, light

skinned, and nonthreatening, preparing white America for the new multicultural citizenship norm.

Like *Time*'s fictitious multicultural citizen, the post-9/11 "face of terror" was a similar sort of fetishized object, but in reverse. "The modern face of terror" was a technologically constructed archetype, and one for which racial categories still deeply mattered despite the absence of overtly racist references. Where the "New Face of America" allegedly represented progress toward an assimilated ideal, the "face of terror" trope deeply negated those same ideals of integration. The face of terror became an imaginary target for directed attention and hatred, but one that was likewise aimed at preparing the United States mainstream for new citizenship norms, especially the intensified practices of surveillance and securitization. Skillfully glossing over the tension between the individualizing and classifying logics of identification—"the tension between 'identity' as the *self-same*, in an individualizing, subjective sense, and 'identity' as *sameness with another*, in a classifying, objective sense"[34]—the "face of terror" trope helped to construct terrorism as a problem with a specific technological solution: computerized facial recognition.



LEFT: "The New Face of America," *Time* magazine's infamous morphed cover image "created by a computer from a mix of several races," November 18, 1993.
RIGHT: "TARGET: BIN LADEN," *Time* cover image close-up of Osama Bin Laden's face, October 1, 2001.

Security Through Intelligence-Based Identification

Precisely how would facial recognition technology be used to identify the faces of "terrorists"? Proponents of the technology were well aware that it was not capable of identifying a "terrorist" facial type, and no credible authority ever made an explicit claim to that effect. In practice, facial recognition systems were being designed to identify individual faces, not classify facial types, an aim most developers would have recognized as a misguided technical goal. Instead, the technology promised to enable the faces of individuals designated as "terrorists" to be identified one by one. Individual faces captured by security cameras in airports and other areas would need to be automatically extracted from images, normalized to conform to a standard format, and digitized to produce mathematical "facial templates." But working systems would depend on more than the digitization of facial images or the installation of biometric capture devices. Significantly, identifying the faces of specific individuals designated as terrorists would also require amassing facial image databases to serve as the memory for automated identification systems. Every individual face to be identified would have to be included in a watchlist database. A massive and complex machinery of vision, built on an enormous image data-banking effort, would be required to make facial recognition systems function for "terrorist" identification.

The policy white paper that Visionics released two weeks after 9/11, *Protecting Civilization from the Faces of Terror*, offered a plan for integrating facial recognition technology into airport and other security systems, emphasizing the critical need for a major intelligence gathering effort to build the terrorist watchlist.[35] The document called for a large-scale initiative, "not only a drastic overhaul of the entire security infrastructure of airports, ports of entry and transportation centers in this country, but also around the world."[36] Under the heading "Security Through Intelligence-Based Identification," the authors outlined five applications for airport security and border control: facial screening and surveillance; automated biometric-based boarding; employee background screening; physical access control; and intelligence data mining. The white paper defined automated facial recognition as an already functioning technology, but one that required more "intelligence" in the form of knowledge of terrorist identities and photographs of their faces. Stopping short of providing the criteria for the designation of individuals as "terrorists," the authors enlisted "intelligence agencies around the world" to take responsibility for building these databases of terrorists' faces, which could then be used "to track them through computerized

facial recognition as they travel from country to country." Once databases of terrorist faces were built from "covert photos and video footage supplied by operatives in the field," they could be networked together to provide an archive of terrorist identities for matching against facial images captured at airports and ports of entry to the United States. According to the company, the Visionics FaceIt system, then in the "deployment phase," would make it possible "to rapidly, and in an automated manner, use video feeds from an unlimited number of cameras and search all faces against databases created from various intelligence sources and formats," and then notify security or law enforcement agents in real time when the system located a match.[37] The watchlist database would be at the center of an effective, functioning facial recognition system for terrorist identification.

Long before the emergence of the database form, image classification systems, enshrined in physical archives, played a central role in the application of photography to the procedures of official identification. The role of the archive and archival practices gained importance with each innovation in photographic reproduction. As Allan Sekula has argued, in the application of photography to criminal identification systems in the nineteenth century, the camera alone was a limited technology.[38] The contribution of photography to identifying criminals came with its integration into a larger ensemble, "a bureaucratic-clerical-statistical system of 'intelligence.'"[39] The central artifact of criminal identification was not the camera, according to Sekula, but the filing cabinet. Sekula foregrounds the central role of the photographic archive as an apparatus of truth production in the Foucauldian sense. Archival systems organize and categorize the visual in ways that do not just reflect preexisting classification schemes but actually create them in the archiving process. Sekula describes the photographic archive as a "clearinghouse of meaning."[40] It "liberates" photographs from the context of their original use, offering them up for a greater number and variety of future uses. It allows new meanings to supplant the meanings derived from the original contexts in which photographs were taken. Yet archives also establish an order on their contents, operating according to an empiricist model of truth.

The electronic database form has inherited these characteristics and in many ways amplified them. The database differs from the conventional archive because it allows the user to access, sort, and reorganize hundreds, thousands, and sometimes millions of records, and it assumes multiple ways of indexing data.[41] The digital reproduction of information, the screen interface, software technology, and other features of the database form distinguish it from physical filing systems. And as a recent manifestation of the archival

form, the database serves as "a new *metaphor* that we use to conceptualize individual and collective cultural memory," as Lev Manovich has argued.[42] The database functions as discourse, according to Mark Poster, a way of configuring language that constitutes subjects.[43] It is both an abstract paradigm and concrete mechanism for organizing information.

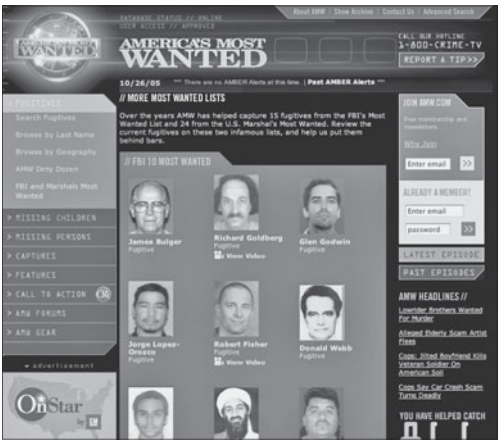
For most of its existence, the database form has been associated with the storage of text-based coded information, but databases are now increasingly used to house visual information as well. Thanks in part to the availability of cheap digital cameras, along with more computer storage and processing power, a veritable "avalanche of images" is flooding into databases. The image database is a cultural form of increasing significance in the organization of visual perception and visual meaning, and a technology that plays a central role in the effort to build computer vision systems. In both their form and content, image databases define the parameters of what computers can be programmed to "see."

Surveillance systems have long been designed to incorporate both visual and text-based forms of information; however, new techniques of digitization, database building, and image retrieval are being designed to provide more effective and automatic ways of processing and organizing visual media, including both still photographs and moving images (including an abundance of images generated from surveillance video). Oscar Gandy has used the term "panoptic sort" to describe a form of "high-tech, cybernetic triage" that uses databases of transaction-generated data to sort individuals according to their presumed economic or political value.[44] Gandy's use of the term "panoptic" is metaphorical—his analysis of the "panoptic sort" emphasized the use of text-based, coded information for the social sorting of people, rather than visual or optical information. But the "panoptic sort" is taking on a more literal, optical dimension along with the growth of image databases and the development of digital techniques of visual image processing. In the case of facial recognition systems, the aim is to translate images of the face into coded information and to automatically connect those coded facial images to text-based, documentary information about individuals. As noted in chapter 1, facial recognition technology promises to more thoroughly and effectively integrate visual and documentary modes of surveillance, which is precisely the innovation that makes it such a potentially powerful technology.

Given that database technology is becoming such an important part of the organization of visual information, how do we visualize the database? What does a database look like? Most likely what we visualize is the software inter-

face, which most directly positions us as subjects relative to a database. Take for example a familiar image of a database-software interface: the screen image of the criminal or "Most Wanted" database. An updated version of the outlaw "Wanted" poster, the Most Wanted database serves an important symbolic function as a cultural image of law and order. The Most Wanted database is a common image in popular crime dramas, for example, where it tends to have fairly extraordinary search capabilities. Screen images that resemble the popular crime drama versions of the Wanted database can be found on the Internet, including one at the website for the television show *America's Most Wanted* (*AMW*) and one at the government website for the FBI.[45] The graphic design of the *AMW* website simulates a crime database interface. On the top of each page, visitors to the site see that their "Database Status" is "Online" and their "User Access" is "Approved." The production values of the *AMW* site surpass the FBI's "Most Wanted Terrorists" website, but otherwise the sites are similar in form. Both display rows and columns of mug shot photographs of wanted individuals, and each digital photo is itself a hyperlink to an individual record with additional information about the wanted person. Navigating these sites invites Internet users to envision themselves as intelligence agents, accessing information about wanted individuals in case of a personal encounter, or doing their patriotic duty to inform themselves about the nation's enemies.

The simulated versions of the Most Wanted database found at these promotional websites convey a particular image of how a watchlist database functions. As much through their design as their content, the sites appear to provide authoritative, unambiguous, empirical information about the



The FBI's ten "Most Wanted" fugitives listed at the website for the television show *America's Most Wanted*. The names and mug shots are hyperlinks to pages containing more detailed profiles on each wanted individual.

identities of the individuals depicted. The screen interface creates a "navigable space" for the database user, and the software enables automated search capabilities, making it easy to peruse the sites, view the images, read about dangerous identities, and even report back to authorities with more information. Web browsers are themselves software interfaces that allow users to access databases that store the contents of the World Wide Web. Using these browsers, we need little or no knowledge of Internet protocols or other technical standards that make the information retrieval methods work to provide us with search results. In fact, web browsers and search engines are explicitly designed to shield users from the complexity of Internet architecture and information retrieval. Most well-designed software interfaces function in this way, as "user-friendly" tools that allow ease of access to and manipulation of data.

But there are drawbacks to the user-friendliness of the software interface. Most significant, the software interface can become a technology of reification, alienating users from the sources of the information they access and the processes involved in information retrieval, especially the algorithmic techniques that determine the relevancy and ranking of information. As a result, the ease of use of the software interface can invest selective search results with a misplaced concreteness. Users become increasingly disconnected from where the data comes from and the decisions that govern what data is available. As Helen Nissenbaum and Lucas Introna have shown, the seemingly neutral process of information retrieval conceals the politics of search engine design, which tends to overvalue certain sources of information, especially those that are already prominent, while rendering other, less visible sources more obscure and difficult to find.[46] Search engine design decisions can have a powerful impact on search results, defining the parameters of relevancy and the range and rank order of information to which users gain access.

In creating "user-friendly" forms of information retrieval, the software interface and database form introduce new layers of mediation between classification systems and end users of those systems. Like physical filing systems, a database embodies and helps to produce a classification system for the information it contains. And while the database might appear to provide an empirical and technically neutral means of classifying and organizing information, in reality every system of classification is itself a process of social construction that involves particular choices and ways of defining and differentiating classes of objects that do not exist *as such* prior to the development of that system. Classification is a technology visibility, a technology

of knowledge and truth production, rather than itself an embodiment of the material reality that it defines and differentiates. Systems of classification "form a juncture of social organization, moral order, and layers of technical integration," as Bowker and Star have argued; they are "artifacts embodying moral and aesthetic choices that in turn craft people's identities, aspirations, and dignity."[47] Classification systems designed into physical filing systems impose an order on their contents in the archiving process. Computerization in turn facilitates the *standardization* of classification systems and their distribution across contexts, multiplying their uses and effects. And as systems become more standardized, the decisions that have gone into devising classification systems recede into the deep structure of technical forms. "When a seemingly neutral data collection mechanism is substituted for ethical conflict about the contents of the forms," write Bowker and Star, "the moral debate is partially erased."[48]

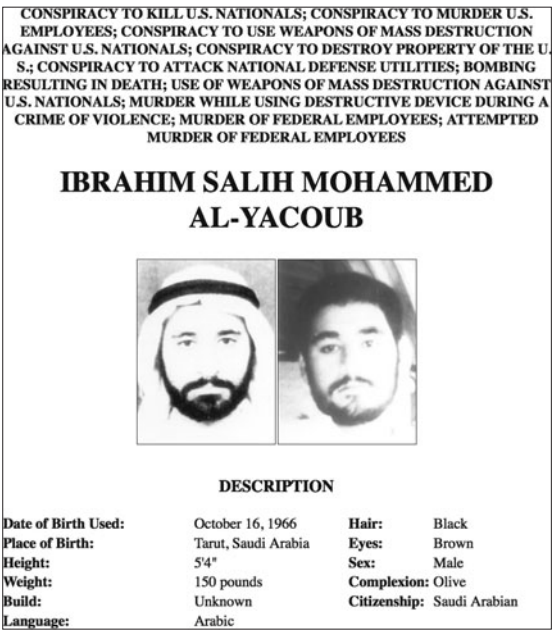
We can begin to see this process of erasure in the way that the *AMW* and FBI websites portray the dossiers of the individuals designated as "most wanted." At these easy-to-navigate websites, the information is presented with authority and simplicity; there appears to be no ambiguity or uncertainty about the identities of the individuals depicted. Clicking on the photograph of a man named Ibrahim Salih Mohammed Al-Yacoub at the FBI website, for example, leads to a page containing the following information in bold, capital letters:

> CONSPIRACY TO KILL U.S. NATIONALS; CONSPIRACY TO MURDER U.S. EMPLOYEES; CONSPIRACY TO USE WEAPONS OF MASS DESTRUCTION AGAINST U.S. NATIONALS; CONSPIRACY TO DESTROY PROPERTY OF THE U.S.; CONSPIRACY TO ATTACK NATIONAL DEFENSE UTILITIES; BOMBING RESULTING IN DEATH; USE OF WEAPONS OF MASS DESTRUCTION AGAINST U.S. NATIONALS; MURDER WHILE USING DESTRUCTIVE DEVICE DURING A CRIME OF VIOLENCE; MURDER OF FEDERAL EMPLOYEES; ATTEMPTED MURDER OF FEDERAL EMPLOYEES.[49]

Just below this information about Al-Yacoub are two black-and-white mug shots, followed by demographic data, a note indicating that he was indicted for the Khobar Towers military barracks bombing, another notifying readers of a five-million-dollar reward, and finally, links to lists of FBI offices and U.S. embassies and consulates. The text presents the identity of this individual in no uncertain terms, and visitors to the site need not question the source

or factual nature of the information presented. Al-Yacoub, as described and pictured, is clearly a "terrorist."

Like the cultural representations of the watchlist database found in popular crime and spy dramas, this particular image of the watchlist database does important work for what William Bogard calls "the imaginary of surveillant control"—creating the powerful image (if not the practical reality) of surveillance system capacity.[50] Although visitors to this website can access specific information about the identities of wanted individuals, this simulated version of the watchlist database performs more of a symbolic than a practical role in the identification of terrorists. The site offers up a set of images of the "faces of terror" for the national imagination, and aims to present an authoritative impression of the intelligence gathering efforts of the state. In addition, while neither the *AMW* nor the FBI website makes use of or even mentions facial recognition systems, both sites do important work in defining a compelling social need for facial recognition technology and speak to its conditions of possibility. They underscore the central role of the watchlist database in the design of terrorist identification systems, and the way that the empirical claims to truth about the database depend to a significant extent on technical design strategies that conceal the underlying complexity, ambiguity, and socially constructed nature of classification systems.



CONSPIRACY TO KILL U.S. NATIONALS; CONSPIRACY TO MURDER U.S. EMPLOYEES; CONSPIRACY TO USE WEAPONS OF MASS DESTRUCTION AGAINST U.S. NATIONALS; CONSPIRACY TO DESTROY PROPERTY OF THE U. S.; CONSPIRACY TO ATTACK NATIONAL DEFENSE UTILITIES; BOMBING RESULTING IN DEATH; USE OF WEAPONS OF MASS DESTRUCTION AGAINST U.S. NATIONALS; MURDER WHILE USING DESTRUCTIVE DEVICE DURING A CRIME OF VIOLENCE; MURDER OF FEDERAL EMPLOYEES; ATTEMPTED MURDER OF FEDERAL EMPLOYEES

IBRAHIM SALIH MOHAMMED AL-YACOUB

DESCRIPTION

Date of Birth Used:	October 16, 1966	**Hair:**	Black
Place of Birth:	Tarut, Saudi Arabia	**Eyes:**	Brown
Height:	5'4"	**Sex:**	Male
Weight:	150 pounds	**Complexion:**	Olive
Build:	Unknown	**Citizenship:**	Saudi Arabian
Language:	Arabic		

Profile page for Ibrahim Salih Mohammed Al-Yacoub, one of the FBI's "Most Wanted Terrorists." http://www.fbi.gov/wanted/terrorists/teralyacoub.htm.

Terrorist Watchlist Database Consolidation

Although the *AMW* and FBI websites perform more of a symbolic than a practical function in the construction of criminal and terrorist identification systems, the records they display are in fact drawn from actual criminal and terrorist watchlists compiled by state agencies to be used for identifying and apprehending targeted individuals. A closer look at the politics of watchlist database building sheds further light on the classifying logic that informs the application of facial recognition technology for terrorist identification. Programming computers to "see" the faces of "terrorists" would require building a database of facial images that would define the parameters of faces a facial recognition system would identify. But building the terrorist watchlist database has turned out to be a challenging prospect, heavily inflected with the practical politics involved in devising classifications and standards, not least those that aim to assign categories of human identity and standardize those categories across populuations.[51] "Whatever appears as universal or indeed standard," write Bowker and Star, is in reality "the result of negotiations, organizational processes, and conflict."[52] The effort to build a terrorist watchlist database provides a special case in point.

The notion that better use of watchlists may have disrupted the activities of the 9/11 hijackers was a common theme in post-9/11 policy discussions. The 9/11 Commission, for example, was dismayed to find that before the attacks, the U.S. intelligence community did not view building and maintaining watchlists as vital to intelligence work. After 9/11, security agencies built out watchlists with a vengeance, investing more labor, more money, and more machinery into the watchlisting effort. Significantly, more people were placed on watchlists, and the terrorist watchlist became an expanding archive of problem identities. Or more precisely, as several federal audits determined, it was an expanding *set* of archives—separate databases dispersed in different locations, compiled and used by different agencies and actors in ad hoc and inefficient ways. Another central problem underlying the intelligence failures of 9/11, according to government reports and policy discussions, was the lack of consistent information sharing among intelligence agencies. The consolidation of the watchlists among various agencies within the Departments of State, Treasury, Transportation, Justice, and Defense became a pressing political priority.

As the Bush White House began to impose a consolidation program on individual security agencies, the challenge and complexity of database consolidation soon became evident. Two years after 9/11, a General Accounting

DEPARTMENTS, AGENCIES, AND THEIR WATCH LISTS

(Twelve separate watchlists maintained by five separate U.S. federal departments, to be consolidated by the Terrorist Screening Center.)

Department	*Agency/Department subcomponent*	*Watch list*
State	Bureau of Consular Affairs	Consular Lookout and Support
	Bureau of Intelligence and Research	TIPOFF
Treasury	Customs	Interagency Border Inspection[a]
Transportation	TSA	No-Fly
		Selectee
Justice	INS	National Automated Immigration Lookout
		Automated Biometric (fingerprint) Identification System[b]
	U.S. Marshals Service	Warrant Information
	FBI	Violent Gang and Terrorist Organization File[c]
		Integrated Automated Fingerprint Identification
	U.S. National Central Bureau for Interpol[d]	Interpol Terrorism Watch List
Defense	Air Force (Office of Special Investigations)	Top Ten Fugitive

Source: GAO.

a. Interagency Border Inspection operates as a part of Customs' Treasury Enforcement Communications System, commonly referred to as TECS.

b. INS is in the process of integrating this system with the FBI's Integrated Automated Fingerprint Identification System.

c. This list is part of the FBI's National Crime Information Center.

d. Interpol (International Police Organization) is an intergovernmental organization made up of 181 member countries for the purpose of ensuring cooperation among the world's law enforcement entities. It is headquartered in Lyon, France. The U.S. National Central Bureau for Interpol, within the Justice Department, serves as the U.S. member of Interpol and facilitates dissemination of Interpol watch list information to federal, state, and local agencies.

Office report found that nine federal agencies were still maintaining twelve separate watchlists, with only sporadic and haphazard information sharing among them. These databases contained a wide variety of data, with no standard or unified set of criteria for who was in the databases, why they were included, or what information about them was retained. Information sharing was hindered by a host of other factors, including not only the "cultural differences" among disparate agencies but also the problem of database incompatibility. The databases of the various agencies were designed for different purposes, by different people, using different software and coding systems, and so were not readily amenable to system integration.

In response to these and other problems, the White House established a new FBI organization called the Terrorist Screening Center (TSC) in September 2003, the latest in a series of consolidation initiatives.[53] The TSC's main purpose would be to develop and maintain a consolidated database, one that had full biometric capabilities and real-time connectivity to all supporting databases. The center would be responsible for making appropriate information accessible around the clock to state and local law enforcement agencies, select private-sector entities, and select foreign governments. By January 2004 the new head of the center, Donna Bucella, testified before the 9/11 Commission that her agency was up and running. Just four months after it was established, the TSC was operating a centralized terrorist database and a twenty-four-hour call center for "encounter identification assistance."[54]

But a Justice Department audit report released over a year later painted a different picture, identifying a litany of problems with the database consolidation effort.[55] The report indicated that the centralized database had a significant number of duplicate records, containing inconsistent and even contradictory information, and that the size of the database differed radically from one phase of development to another. There was a lack of connectivity between the central database and the participating agencies, primarily because many of the agency systems did not support automated data sharing—each of their computer systems would need to be upgraded, which could take years. There were also inconsistencies in the coding of records: for example, over thirty thousand records had "handling codes" that did not correspond to something called their "INA codes." Handling codes indicated what protocols agents should follow in the event of a positive identification with a suspect; INA codes indicated how the individual was associated with international terrorism. Some of the records had handling codes that were too lenient relative to their INA codes, others were too severe, and some of the records had no handling codes at all. The coding scheme in general was

not always appropriate to all the records in the database. For example, there was nothing corresponding to an "INA code" for domestic terrorists (who *were* in fact included in the database), so domestic terrorists were automatically assigned international terrorism codes. Significantly, the consolidated database could store biometric data (such as a photograph), but it did not have the capacity to search based on biometrics, so screening continued to rely exclusively on name-based searches. Some known terrorist suspects were missing from the database, and many records were missing important information.[56] The report also noted that some of the records in the new consolidated database were missing the code that designated their originating agency.[57]

As the lengthy list of problems suggested, the watchlist database consolidation effort was a complex, labor-intensive, and highly imperfect process. The reality of watchlist consolidation ran counter both to prevailing popular conceptions of the watchlist database (like those found in popular crime and espionage dramas, and at the *AMW* and FBI websites), and to the seemingly straightforward industry proposals for large-scale, networked terrorist identification systems. While there was certainly a general awareness of the lack of information sharing among U.S. federal agencies, the extent and complexity of the problem of database building was shrouded in a reified notion of the database as an empirical, truth-telling technology. While the database is of course a powerful technology of truth, its truth-telling capacities depend to a significant extent on the way a database is designed, the assumptions behind the classification system that it embodies, and the specific purposes for and conditions under which it is populated. This is not to say that databases cannot yield unanticipated answers, take new forms, or be applied to unforeseen uses. But database building and consolidation are especially challenging processes, fraught with error and ambiguity. No matter how well executed, the database consolidation process itself would have important consequences for the form and content of the resulting classification system. Rather than merely organizing information and offering a transparent reflection of reality, the database form in fact helps constitute the objects it purportedly represents. And consolidating disparate databases involves standardizing their form and contents, thereby transforming those contents in the process. As the head of the Terrorist Screening Center said in front of 9/11 Commission, the individual databases of different intelligence agencies "were created to support the mission of the individual agencies, [they] are in many instances, their case management systems, not terrorist watch lists."[58] In the transfer of data from uniquely devised "case management systems"

to the consolidated watchlist, new terrorists were born. What was a "case" particular to an agency investigation became a more generalized "terrorist identity."

In short, one of the most problematic effects of terrorist watchlist expansion and consolidation was a broadened definition of "terrorist" to include a diverse array of problem identities. Like the archive before it, the consolidated watchlist database liberated individual records from the context of their original use, offering them up for new meanings and new uses in the "war on terror." At the same time, the database operated according to an empiricist model of truth, so that this transformation of meaning and use was construed as a technical matter of engineering a more efficient and logical information architecture. The twice-removed status of individual records in a *consolidated* watchlist left the new uses of the archived identities that much further from the context of their original designation as a terrorist or other problem identity. Watchlist database consolidation rendered the "terrorist" designation in technical form, rationalizing and instrumentalizing it as a matter of technical procedure. And the deployment of an ostensibly objective definition of the terrorist identity occurred under the veil of empiricism and technical neutrality that the image of the database afforded.

Seeing the Faces of Terrorists

The difficulties with the terrorist watchlist database consolidation effort underscore the persistent problems involved in building stable identification systems, pushing standardized identity categories back out into the world in order to differentiate populations according to categories of privilege, access, and risk. In spite of every effort at stabilization, argues Jane Caplan, identification systems are fundamentally unstable, precisely because their purpose is to stabilize the inherently unruly concept of identity.[59] Photography was originally applied to identification systems in an attempt at stabilization and modernization, to help visually bind identities to faces and bodies in order to control for the subjective, interpretative, imperfect, and highly variable ways that human beings looked at and identified one another's faces. Automated facial recognition is designed to further assist, and even replace in some cases, the subjective human practice of facial identification, again with the aim of standardizing identification systems and stabilizing human identity. But as the inescapable archival basis of this process suggests most acutely, the instability of identity cannot be resolved through additional layers of technical integration. "Even in its most controlling and technologized

forms," identification is "based on a concept that is itself difficult to stabilize and control"—the concept of *identity*.[60]

Despite the seemingly unambiguous ways in which post-9/11 security discourse wielded the trope of the "terrorist" or the "face of terror," there is perhaps no category of identity as unruly and unstable as that of the "terrorist," a fact that comes into sharp relief in the case of the terrorist watchlist consolidation effort. Devising a consolidated watchlist database for terrorist identification was a biopolitical project, one that inescapably bound the security of the population to the state's sovereign claim to the right to kill. Killing here meant not just to literally murder people but also to increase the risk of death for some people, inflicting "political death, expulsion, rejection, and so on."[61] Although automated facial recognition has not quite materialized as a functioning technology for terrorist identification, it nevertheless promises to facilitate precisely these biopolitical aims, working with expanding databases of mug shot images. But regardless of whether individuals designated as terrorists can be identified using automated forms of facial recognition, the *virtual* face of terror serves a key biopolitical function, brandished as a weapon to justify state racism and define the war on terror as a virtuous one.

The drive to stabilize identity by automating the perceptual labor of identification connects innovations in identification systems with debates about the nature of visual perception and its relationship to photographic technologies. Scholars of visual culture have debated at some length the implications of new visual media technologies for our understandings and experiences of sight and vision. Does the automation of vision open up our experience of the visual world to new possibilities, or is machine vision having repressive and even blinding effects on how we see the world? Paul Virilio has perhaps the bleakest diagnosis.[62] In the drive to automate visual perception, he sees inherent imperialistic and militaristic impulses. The technologies of war and cinema have been developed in concert, enabling both the visual augmentation of military logistics as well as the militarization of societies and their mobilization for war. If machines can "see" in Virilio's analysis, they have a frightening tendency do so with an eye for bloodshed. Kevin Robins similarly sees inhuman and inhumane propensities in new visual media technologies. For him, they embody a desire to disavow the reality of the world's events and place distance between people and the worlds they inhabit. "Technologically mediated vision," writes Robins, "developed as the decisively modern way to put distance around ourselves, to withdraw and insulate from the frightening immediacy of the world of contact."[63] Automation goes hand in

hand with the rationalization of vision, according to this view, and the development of prosthetic visual devices separates visual perception from the natural capacities of the human body. The "relentless abstraction of the visual" through computerized imaging technologies has involved "relocating vision to a plane severed from a human observer," robbing humans of their privileged status as perceiving subjects.[64]

Others take a different view of technologically enhanced vision. John Johnston has argued that critics like Virilio wrongly assume a stark opposition between the human and the technical, and this assumption imposes limits on reflection about vision and visual culture.[65] Johnston does not believe that human vision can be opposed to machine vision, instead using the Deleuzian concept of "machinic vision" to theorize "an environment of interacting machines and human-machine systems," as well as "a field of decoded perceptions that . . . assume their full intelligibility only in relation to [machines]."[66] In other words, new human-machine assemblages create new possibilities for the subjective experience of sight, for what vision means and how it works, and for how humans and machines collectively see the world. Donna Haraway similarly argues that humans are already inescapably embedded with visual media technologies. It is in the intricacies of these embedded relationships between humans and technologies, she argues, "that we will find metaphors and means for understanding and intervening in the patterns of objectification in the world, that is, the patterns of reality for which we must be accountable."[67]

Johnston and Haraway are right to argue that human visual perception is inescapably integrated with technical forms, that visual forms of perception are constituted not by human bodies alone but through assemblages of human vision, visual devices, and techniques of observation. But whether humans will ever use the changing vantage points afforded by new forms of "machinic vision" to see the world differently remains to be seen. In the process of designing new technologies of vision, our subjective forms of visual perception are themselves being reinvented. What seems cause for concern about this process is how rarely (if ever) it leads to radically new ways of seeing, instead reinscribing, in more effective ways, existing power relationships and dominant modes of vision. Any celebration of the radical possibilities opened up by new human-machine visual assemblages must be tempered by a recognition that a certain set of institutional actors and their constituencies are the primary agents and beneficiaries of emergent forms of "machinic vision." It may in fact be misguided to hold out a nostalgic attachment to the natural capacities of human perception unadulterated by mediated

forms. But it is likewise mistaken to turn a blind eye to what are clearly the dominant forms of human-machine perception, forms that incorporate and authorize very particular ways of seeing the bodies and faces of others.

In their development and practical applications, automated facial recognition systems make use of socially constructed classification systems for defining and standardizing identity categories. Formalizing these classification systems, amassing databases of facial images, and implementing new identification technologies are institutional projects being undertaken mostly by state agencies, law enforcement actors, and business entities. But there are also ways in which these projects and their associated practices are taking shape at the level of the individual, imported into the realm of everyday practice for a certain class of security-conscious, tech-savvy citizens. Individual users are participating in the project of facial image database building, taking photographs of faces, storing them in databases on their computers, and migrating them online. They are also being invited to participate in the development of facial recognition technology by experimenting with software prototypes designed for individualized use. The next chapter examines how the securitization of identity is imported into the self-fashioning activities of tech-savvy individuals through the introduction of consumer applications of facial recognition technology.