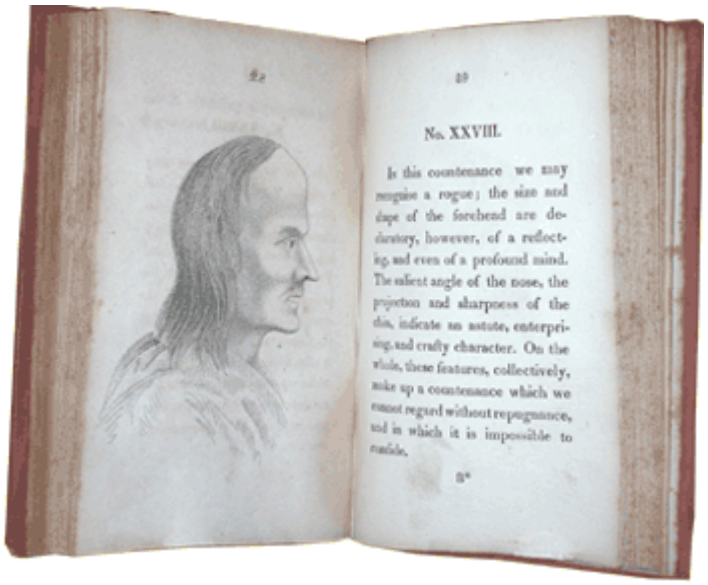
The Physiognomy of Biometrics: The face of counterterrorism



Terror is not faceless.

—Joseph Atick, CEO Identix, 2002

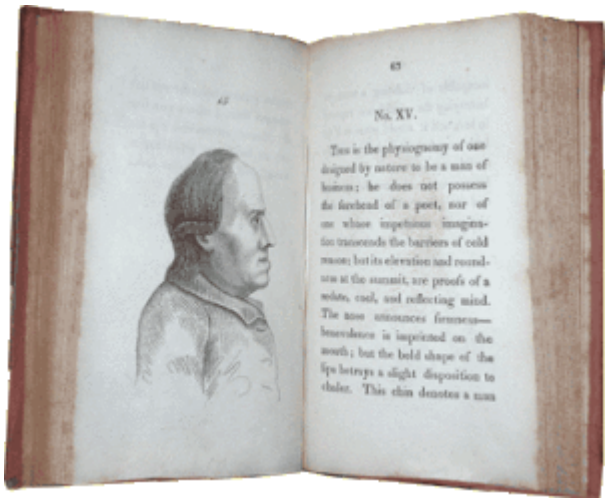
I.

Susanna Rowson's postrevolutionary novel *The Inquisitor, or Invisible Rambler* (1788, 1793) recounts the experiences of a wealthy gentleman who, after complaining about the amount of duplicity in the world, is mysteriously given a ring that can turn him invisible. With the power of invisibility, the gentleman boasts that now "I should find my real friends, and detect my enemies." And that is more or less what happens. Over the next three volumes of the novel, the gentleman's morning walks provide him with numerous occasions to use his invisibility for the benefit of mankind. He exposes rakes, protects the innocent, and saves lives from ruin. Sometimes the gentleman intervenes after witnessing an immoral act while invisible, but far more often he first suspects someone and then investigates the person's behavior invisibly. His ability to follow the duplicitous before they execute their designs is integral to the novel's imagination of social order and justice. Yet, if his invisibility is what enables him to spy on people unobserved, then how does he know whom to watch and whom to ignore?

He knows, we later learn, because he is a physiognomist. "I never cast my eye upon a stranger but I immediately form some idea of his or her dispositions by the turn of their eyes and cast of their features," he explains, "and though my skill in physiognomy is not infallible, I seldom find myself deceived." Indeed,

nearly all of the people the invisible rambler suspects eventually behave as their faces predicted they would. Throughout *The Inquisitor*, faces reveal seducers, gamblers, idlers, dissimulators, and a variety of crooks and fortune hunters. For Rowson at least, a person's face becomes the probable cause for the rambler's surveillance.

The idea that a person's face could belie his will and disclose his character can be traced to Johann Lavater's enormously popular *Essays on Physiognomy* (1775-78). At least twenty editions of Lavater's *Essays* were published in English, including two in America, before 1810. By 1825, American periodicals had featured no fewer than seventy articles on physiognomy. Lavater's distinction between *pathognomy* (the study of man's passions and his visible, but impermanent facial expressions) and *physiognomy* (the study of the correspondence between man's moral character and his permanent and unalterable facial features) limited the power of people to manipulate the reception of their image in public, since it disassociated expression from character. Since Lavaterian physiognomy read moral character from unalterable and involuntary facial features, it created a visual system for discerning a person's permanent moral character despite his or her social masks. Readers of the 1817 *Pocket Lavater*, for instance, learned how to look at the features of various white male faces in order to discriminate "the physiognomy of . . . a man of business" from that a "a rogue."


63

No. XV.

This is the physiognomy of one designed by nature to be a man of business: he does not possess the forehead of a poet, nor of one whose inquisitive imagination transcends the barriers of cold reason; but its elevation and roundness at the summit, are proofs of a sedate, cool, and reflecting mind. The nose announces firmness—benevolence is imprinted on the mouth; but the bold shape of the lips betrays a slight disposition to chider. This chin denotes a man

The Man of Business, opposite page 63 in Johann Caspar Lavater, The Pocket Lavater, or, The Science of Physiognomy (New York, 1817). Courtesy of the American Antiquarian Society.

By turning to physiognomy as a way to detect vice, expose dissimulation, and undermine social mobility in their novels, Rowson and other postrevolutionary authors reproduced Lavater's opposition between a model of character read from performance and one read from the structure of the face. In contrast to the revisable, performed, and voluntary self of the fortune-hunting seducer Cogdie, for instance, *The Inquisitor* posits the permanent, physiognomic, and involuntary one used by the invisible rambler to unmask him. This opposition

was foundational, I would argue, to how the postrevolutionary novel in particular and early American culture in general imagined the structure of social relations. The physiognomic distinction of the face opposed the functional, almost incidental relation of a person's body to genteel performance that texts such as Benjamin Franklin's *Autobiography* promoted and, as a result, it challenged Franklin's idea that the acquisition of his social and political power was as universally available as the acquisition of his conduct. With the rise of physiognomy, the sphere of agency from which a person's moral character could be known shrunk from the range and quality of his actions to the contour and shape of his face.

I begin with *The Inquisitor's* invocation of physiognomy and surveillance to "find my real friends, and detect my enemies" because its attention to the face, social goals, and underlying logic are similar to those now surrounding today's science of biometrics (which includes but is not limited to facial recognition systems). This is not to say that biometrics and physiognomy are the same. When biometrics look to a face it is to identify a person, when physiognomy looks to a face it is to identify that person's permanent moral character. Yet, each attempts to control mobility and the instability it brings to the social order by turning to bodies in general and faces in particular. These two sciences, eighteenth-century and twenty-first, share, in other words, a commitment to the idea that the body does not change, and they seek to ground a person's essential character or unique identity in that idea of the body's permanence. In so doing, however, both insist on a false opposition between a model of character that is performed and one that is corporeal. The persistence of this opposition may help to explain why the failure of biometrics to provide security seems to have no bearing on the perception that they provide security nonetheless.

II.

Biometrics are often associated with the future. Facial recognition systems, fingerprint readers, and retinal scans are the stuff of science fiction films such as *Total Recall* and *Minority Report*. Yet, as you read this, they are becoming very much a part of the present. Next year, the Enhanced Border Security and Visa Reform Act of 2002 will require that all visas and other travel documents to the United States include biometric identifiers. A $10 billion border control contract has already been awarded and plans are underway to install biometric devices (most likely fingerprint and facial recognition systems) at all three hundred border entry points. Soon biometrics will also be used to identify some two million transportation workers. Last year, the Department of Homeland Security handed out nearly $11 billion for biometrics, and it seeks another $1.4 billion in 2005. Millions more have been spent by the Department of Defense. Earlier this year, the American Association of Motor Vehicle Administrators upped the ante by proposing to create the world's largest database of biometric data: a North American ID card that would utilize approximately three hundred million DMV facial images. Most recently, the 9/11

Commission report urged the government to establish a comprehensive biometric screening program “as quickly as possible.” These are but a few examples of what can only be called a stampede of post-9/11 government legislation, projects, and contracts all looking to buy what the biometric industry is selling: security. With over two hundred vendors now offering biometric solutions, the International Biometrics Group predicts that global revenue from biometrics firms will climb to $4.64 billion by 2008.

So how does biometrics provide security? Most biometric technologies automate the identification of people by one or more of their distinct physical characteristics, matching a face or a fingerprint, for example. As Michigan State University engineering professor Anil Jain explains, biometrics rely on who you are as opposed to what you know (such as a password) or what you have (such as a passport). They transform a unique personal feature such as your face into a numerical code or template, store that template, and then compare your face to it each time thereafter. In short, biometrics turn your body into your password. Biometric systems either prove that you are who you say you are (verification) or they prove that you are not who you say you are not (identification). During verification, your face is matched with your template so that you are positively identified. During identification, your face is compared against every face in a database (such as a gallery of terrorists) to insure that you are not on a watchlist. Since biometrics claim to be more difficult to copy, forge, share, lose, or forget than traditional credentials, they have been heralded as an almost infallible way to control access to secure areas.

Biometrics, however, can make mistakes. A false match happens when you are incorrectly matched to another person’s template (as would be the case if you were falsely identified for a terrorist). A false nonmatch occurs when a person is incorrectly *not* matched to a truly matching template (as would be the case if you were not identified as yourself). Now here is the rub: you cannot lower both error rates simultaneously. The more you try to reduce the chance of people being falsely identified as terrorists, the more likely they will not be identified as themselves, and vice versa.

This has proven to be quite a problem for the industry, since biometrics, especially facial recognition systems, have not performed well when tested. A recent National Institute for Standards and Technology study, for example, found that facial recognition technology failed to match people correctly 23 percent of the time. Last year, it failed to match employees at Boston’s Logan International Airport up to 38 percent of the time, and in 2002 it failed to match Palm Beach Airport employees 53 percent of the time. According to the*Economist*, the 2003 government-sponsored Face Recognition Vendor Test found that “none of the systems worked well . . . when shown a face and asked to identify the subject.” Martyn Gates, a facial recognition specialist, confessed to the *Financial Times* that “in some systems, the accuracy is almost random.”

No. XXVIII.

In this countenance we may recognise a rogue; the size and shape of the forehead are declaratory, however, of a reflecting, and even of a profound mind. The salient angle of the nose, the projection and sharpness of the chin, indicate an astute, enterprising, and crafty character. On the whole, these features, collectively, make up a countenance which we cannot regard without repugnance, and in which it is impossible to confide.

The Rogue, opposite page 89 in Lavater, The Pocket Lavater. Courtesy of the American Antiquarian Society.

Part of the reason biometrics perform so poorly, as many industry experts admit, is that the technologies are still immature. Consequently, biometrics have been routinely fooled or “spoofed.” Magazine photographs and high-resolution images of faces have been enrolled into facial recognition systems, while cadaver, silicone, and gelatin fingers have fooled fingerprint scanners. As the *Wall Street Journal* reported last year, Tsumoto Matsimoto from Yokohama University was able to fool eleven different fingerprint scanners roughly 80 percent of the time using $10 worth of gelatin. Researchers at West Virginia University, the *Guardian* noted, were able to enroll fourteen cadaver fingers into a biometric system and, once enrolled, were able to verify their identities 40-94 percent of the time. Yet, you do not have to try to “spoof” biometrics in order to generate errors. Head movement, skin color, lighting conditions, and camera angles all affect the accuracy of facial recognition systems. Similarly, finger placement, hand lotion, dust, humidity, and temperature can alter fingerprint scans.

III.

Although biometrics does make forging credentials more difficult, a person’s biometric data can still be stolen. A 2003 National Academies of Sciences report, for example, recommended that “biometrics should not be sent over a network” because the transmission of templates to a remote database presents the risk of theft. Yet, “the biggest reason biometrics are vulnerable to misuse,” the NAS report warned, “is that, unlike computer passwords or bankcard PIN numbers, they’re not secret.” “Collecting the data needed to compromise a person’s bioprint,” David Hamilton observed in the *Wall Street Journal*, “may be no more complicated than spying on him for a day or two” before lifting a fingerprint from a glass. And “once someone steals your biometric,” security expert Bruce Schneier explains, “it remains stolen for life.” While the government can issue a new passport or a bank, a new PIN number, a person has only one face and ten fingers.

Even if biometric technology were infallible, critics maintain that it violates a person's right to privacy and compromises our ability to live in a free society. Stephen Kent, committee chairman for the NAS report on biometrics, warned, "The ability to remain anonymous and have a choice about when and to whom one's identity is disclosed is an essential aspect of a democracy." Others worry about what sociologists call "function creep," the process by which information is used beyond its initial intended and limited use. The ease with which facial recognition systems have been integrated with closed circuit television cameras or other third-party databases has alarmed civil liberties and human rights activists, who are concerned that biometrics would lead to the creation of a global surveillance infrastructure. "Without social agreement and legal restrictions on how the system could be deployed," George Washington law professor Jeffrey Rosen imagines, "it could create a kind of ubiquitous surveillance that the government could use to harass its political enemies or that citizens could use, with the help of subpoenas, to blackmail or embarrass each other."

If 9/11 sparked the biometric boom, there are doubts about how effectively the technology can identify future terrorists. As one critic put it in the *New Scientist*, "I could give you my fingerprint and you still wouldn't know who I am. Biometrics says nothing about whether I'm a terrorist or not." Indeed, all nineteen of the 9/11 hijackers entered the country using valid visas, on their own passports. "Verifying their identities using biometric visas," the *Economist* recently argued, "would have made no difference." Even though photographs of known terrorists can be enrolled into facial recognition systems, only a few terrorists have ever been identified, and those images are often blurry and unreliable. Others contend that terrorists could exploit human error during the nontechnological process of enrollment. As technology specialist Keith Rhodes warned Congress, "[B]iometrics cannot necessarily link a person to his or her true identity . . . People who are not on the watchlist cannot be flagged as someone who is not eligible to receive a credential."

IV.

With the *Wall Street Journal* calling facial recognition technology "one of the most error-prone types of biometric devices available today" on the one hand, and the ACLU branding it "an over-hyped failure" on the other, how can the government's continued appetite for biometrics and the public's apparent indifference to its costs and problems be explained? "It is difficult to avoid the conclusion," the *Economist* told its readers, "that the chief motivation for deploying biometrics is not so much to provide security, but to provide the appearance of security." Yet, poll after poll reveals that a majority of Americans believe that biometric screening will increase security. Why do so many find an illusion sufficient for security?

Without debating the strategic merits of the deterrent value of biometrics in a post-9/11 world, the confidence displayed in biometric technologies might have

something to do with how they recall familiar but ultimately unproven ideas about the body's permanence and its capacity to communicate our essential moral character or our unique identity. Biometrics posits that there are unique, measurable, and permanent physical features, which is why this science—like physiognomy before it—has difficulty with the simple fact that people change. Aging, weight gain or loss, changes in hairstyle, illness, accident, and cosmetic surgery have all been found to alter presumably permanent biometric characteristics. "Biometric input is not always the same and the technology has difficulty adapting to input variations," admits Valorie Valencia, CEO of the biometric firm Authenticorp. In fact, the problem of user change is significant enough that the euphemistically labeled "time decay" of each kind of biometric is now part of a $3.1 million NSF/DHS study. By insisting that there are permanent features of the face, biometrics reproduce the physiognomic fallacy: namely, that there is an opposition between a voluntary, revisable self knowable from behavior and an involuntary, permanent self knowable from the body. Moreover, just as physiognomy was imagined by postrevolutionary novelists such as Rowson to thwart the rapid social mobility of fortune-hunting seducers, biometrics imagine the permanence associated with the corporeal self as an instrument for identifying people and regulating their mobility.

The disavowal of the physiognomic fallacy by the biometric industry perhaps can be most strongly felt in how it chooses the future rather than the past in order to confront questions about the social consequences of its technology. In general, the industry and the media covering it address the social effects of biometrics as they are imagined in blockbuster Hollywood films such as *Minority Report*, *The Bourne Identity*, or *Enemy of the State*. (Industry experts served as technical consultants to many of these films.) At last year's Biometric Consortium Conference, for instance, Catherine Tilton blamed Hollywood depictions of biometrics for perpetuating a series of myths regarding the loss of privacy, the loss of freedom, constant surveillance, absurd costs, and inaccuracy of biometrics. Chris Winton of Biometrics Australia lodged a similar complaint this year to the *Sydney Morning Herald,* saying that "biometrics is suffering from bad PR as a result of Hollywood."

Illustration from Johann Caspar Lavater, Essays on Physiognomy: For the Promotion of the Knowledge and the Love of Mankind (Boston, 1794). Courtesy of the American Antiquarian Society.

By pointing to Hollywood dramatizations of biometrics as the origin of "myths" regarding the technology's violation of privacy and freedom, the industry denies the actual, relevant histories of identity and corporeality that have existed in the United States and elsewhere since at least the era of physiognomy. It puts biometrics in dialogue with futuristic fantasies—at times paranoid, at other times, accurate—about its imagined social effects rather than with actual past histories of the social, cultural, and political consequences of identifying people by their bodies. When the past is invoked by biometrics, its official genealogy is a progressive, scientific one beginning in the late nineteenth century with the early biometric criminologists, Alphonse Bertillon (inventor of a body measurement system for identifying criminals) and Francis Galton (father of fingerprinting), and evolving to the technologically savvy and precise biometrics of today. On the one hand, biometrics desires a history, but on the other, it suppresses its own relationship to prejudicial scientific discourses such as physiognomy, phrenology, anthropology, Bertillonage, and eugenics and their histories of generating and naturalizing social types complicit with racism, discrimination, and social injustice.

These histories seem particularly important to consider given the nontechnological aspects of biometrics. The question of how to identify a terrorist without a picture of his face, for instance, remains unanswered by biometrics, and the mysterious notion of a "watchlist" only defers the issue to government intelligence. How the watchlist is constructed, who is on it, and for how long, are rarely addressed in the debate over biometrics. When asked if he knew, Raj Nanavati of the International Biometric Group told *Newsweek*, "I'm not sure myself . . . they're comparing it against a watchlist of nondesirables." While biometric boosters like Identix CEO Joseph Atick assure

the public that “trusted identity . . . is not a class distinction,” his own description of how his company’s facial recognition system will be able to discern the untrustworthy few from the “trusted identity” of “the honest majority” sounds all too similar to the invisible rambler’s magical declaration to “find my real friends, and detect my enemies.”

Further Reading:

The emerging field of biometrics has produced a large number of short, mostly informative Web, newspaper, and periodical sources, but only a few book-length examinations. For more information on biometrics, see Joseph Atick, “Biometric Consortium Keynote Speech,” Biometric Consortium, Washington D.C., Feb. 2002; Ruud M. Bolle, Anil Jain, and Sharath Pankanti, “Biometrics: The Future of Identification,” *Computer* 33:2 (Feb.2000): 46-49; Owen Bowcott, “Biometrics Helping the Fight Against Terror, Hindering the Hope for Privacy,” *Guardian*, 18 June 2004, 3; David P. Hamilton, “Workplace Security (A Special Report); Read My Lips: Are Biometric Systems The Security Solution of the Future? Maybe, But We’re Not There Yet,” *Wall Street Journal*, 29 Sept. 2003, R4; Anil Jain, Sharath Pankanti, and Sailil Prabihakar, “Biometric Recognition: Security and Privacy Concerns,” *IEEE Security and Privacy*, 1:2 (March/April 2003): 33-42; *The Nine-Eleven Commission Report*, Washington D.C., 2004; Christian Parenti, *The Soft Cage: Surveillance in America: From Slavery to the War on Terror* (New York, 2003); Jeffrey Rosen, *The Naked Crowd* (New York, 2004); Irma Van der Ploeg, “The Illegal Body: ‘Eurodac’ and the Politics of Biometric Identification,” *Ethics and Information Technology* 1 (1999): 295-302; and James Wayman, “Interview with Joe Palca,” *Talk of the Nation*, National Public Radio, 11 June 2004. For more on physiognomy at the end of the eighteenth century, see Johann Caspar Lavater, *Essays on Physiognomy*, trans. by Henry Hunter, with engravings by Thomas Holloway, 3 vols. in 5 (London, 1789-98); Johann Caspar Lavater, *The Pocket Lavater or, The Science of Physiognomy* (New York, 1817); and Susanna Rowson, *The Inquisitor, or Invisible Rambler* (1788; Philadelphia, 1793).

This article originally appeared in issue 5.1 (October, 2004).

Christopher Lukasik is an assistant professor of English and American studies at Boston University. He is currently completing a book manuscript entitled, *Discerning Characters: Social Distinction and the Face in American Literary and Visual Culture, 1780-1850*.