social security numbers. As genetic material, it provides the opportunity to incorporate statements about character, intelligence, and disposition. Exploiting DNA in this way will both draw on eugenic, racist theories popular during in the early to mid-twentieth century, and will provide them with a new legitimation.

16

Under My Skin: From Identification Papers to Body Surveillance

DAVID LYON

A RUSSIAN PROVERB says that humans may be thought of as "body, soul, and passport" and a few years ago I suggested this be updated to "body, soul, and credit card."[1] The point, of course, is that documenting individual identity underwent a shift in the twentieth century, from predominantly print-based information required by the state, to the proliferation of electronically stored data required by commercial businesses. In this essay, however, I want to consider what might be thought of as a return to the "body and soul" definition, although the latter has little or no significant role either. This is not a contraction of demands for identification so much as the co-opting of the body itself as a means of identification. Those intricate lines that form a fingerprint, the geometry of hands, thumbs, or fingers, and the patterns of cones and rods on the retina are the most common candidates for what might be termed "body surveillance." To these may be added voice modulations and images of the face, and genetic clues that may be gleaned from body fluids. Such identification relies on electronic databases, and still relates in part to the state, but its implications take us well beyond the world of passports and credit cards.

In the last part of the twentieth century, a subtle shift began to take place. The body became, once again, a source as well as a site of surveillance. I say "once again," because there is nothing intrinsically new about the body being used in this way. Over a hundred years ago, criminal anthropometry claimed that body shapes, especially the head, could spontaneously reveal the unlawful proclivities of the person. Today, the development of new biometric technologies means that the body itself can be directly scrutinized and interrogated as a provider of surveillance data. Information for identification may now be extracted from the body that can override the person's own claims to a particular identity. And data originating in the body is used for the same kinds of purposes as more

[1] Lyon 1994: 3.

conventional modes of surveillance, to sort and classify, to determine eligibility, to qualify and to disqualify, to include and to exclude. The body need no longer merely be watched to track its behavior or its whereabouts. Surveillance now goes under the skin to monitor, check, and test in order to identify and to classify. The subtle shift is one of technological sophistication in body surveillance, and its broadened use from potentially criminal to general populations of citizens and consumers.

From the birth of modernity, the body achieved new prominence as a site of surveillance. Bodies could be rationally ordered through classification in order to socialize them within the emerging new nation-state. Bodies tended to be distrusted as sensual, irrational, and thus in need of taming, of disciplinary shaping to new purposes.[2] By associating a name or, later, a number with the body, each person could be distinguished from the next. Thus if, for example, a name appears on a voters' list, and if an embodied person shows up to record a vote, then the citizen can be recorded as having voted, after which that person may not vote again. Similarly, citizens of modern nation-states are required to carry all manner of personal identifiers that ensure their smooth passage through benefits offices or customs and immigration departments. Papers and cards are part of the essential personal paraphernalia of modern life.[3]

In these cases, however, the means of identification is external to the body. Indeed, the volatile and unpredictable body is put in its place by the cognitive focus on the name or the number. This situation still obtained during the period of large-scale bureaucratic computerization from the 1960s on. Although at some point it might be necessary to ask the person to identify herself verbally, the trend set in train with computerization was toward the automated cross-checking of identity. Trustworthy third-party sources could be enlisted to ensure that the individuated person was indeed eligible for benefits or qualified to drive a car. Thus a web of first documentary, and then digital identification systems could locate and distinguish individuals when required. It was often almost incidental that a body was also associated with the person whose identity was being checked. The number and name were what really mattered.

But computerization was to bring other issues in its train, especially as communication and information technologies (CITs) make possible the almost instantaneous transfer of documents and and financial, medical, or other sensitive information. The ease with which these can be intercepted by third parties has generated what the U.S. Public Interest Research Group calls "identity theft," said to be the "fastest growing crime

[2] Mellor and Shilling 1997: 147.
[3] See Lyon 1994: 3–21.

in the nation."[4] It occurs in various ways, including at automated bank machines, through e-mail that uses others' addresses, by sending false messages on the Internet, or by breaking into computer systems to gain access to personal data. Various forms of encryption that provide digital signatures or pseudonyms have proliferated as means of combatting such "identity theft." They are often referred to collectively as "Privacy Enchancing Technologies," or PETs.

The quest for accuracy and precision continues, however, and now other new technologies are enlisted as adjuncts to the computer. These techniques are known generically as "biometrics" because they refer to measuring or monitoring parts of the body. In 1998, for instance, the Nationwide Building Society in the United Kingdom tested iris-scanning equipment at some of their automated bank machines.[5] The concentrated wealth of features in the iris makes it an ideal candidate for automated identification. But the human fingerprint also remains popular as a means of identification, especially since the capacity of digitized print images has grown greater, and costs have fallen. Its uses range from a traffic control system in Shaanxi Province of Central China, where smart cards holding drivers' records are verified by stored fingerprints,[6] to a "BioMouse" that uses fingerprints as passwords into laptops or computer systems.[7] Hand scanners serve similar purposes, for example, allowing only authorized users to work out in the University of Montreal's athletic complex.[8]

Several significant issues are raised by this. I begin by charting the background to body surveillance, in various kinds of documentary and digital identification. This social-historical account serves to show how the new biometric technologies are given their chance. Although enabled by computerization, body surveillance represents a merging of techniques not previously thought of as "information" technologies. Despite their relative novelty, however, these new techniques are appearing in all surveillance sectors. They are seen in government administration, and in policing, but also in the workplace and consumer spheres. In each sector, moreover, it is important to examine the implications of body surveillance for reconfigured relations of time and space, for the boundaries between the public and the private, and for the interactions between technology and society. Lastly, I return to the central issue of the body as a "document" for identification, and what this means for surveillance in a world of identity politics and risk management.

[4] U.S. Public Interest Research Group 1996: 14, cited in Cavoukian 1997.
[5] Pearsall 1998: 11.
[6] Kirbyson 1996: 6.
[7] Guly 1997: 23.
[8] Beiser 1997: 40.

Identity, Identification, and Modernity

Recognizing a person's separate identity depends on three things; a body, a memory, and rights and responsibilities. Erving Goffman, in his classic work on *The Presentation of Self in Everyday Life*,[9] stressed the importance of the face and the body for recognition and everyday encounters. A person is an ineluctably social being; individuals are "embodied social agents."[10] We require the recognition of others to be identified as individuals. But the body does not suffice on its own. We must also give an account of ourselves that confirms our identity, and must also be committed to that story. This authorizes our past as truly ours. Beyond this, a person's identity is also bound up with social expectation; agents are responsible for their actions. A growing emphasis of the modern world, paralleling the focus on responsibility, has been to attribute rights to individuals, to which they or others may appeal in law.

In early modernity, as Nicholas Abercrombie and others point out, the long, drawn-out discovery of the individual had contradictory consequences. "As individuals become more separate and different, they are more recognizably unique. In turn, uniqueness and identity are closely connected and the identification of individuals makes their control that much easier."[11] How did this happen? The coming of modernity meant that individuals were granted an increasing range of rights, starting with civil rights before the law, and moving to political rights of citizens, and social rights to welfare. But to obtain these rights, bureaucratic structures required careful scrutiny of the grounds of entitlement according to consistent rules. So people had to be registered, and their personal details filed, which of course paradoxically facilitated their increased surveillance. Freedom from one set of constraints—those of feudal societies—gave opportunities for new forms of surveillance and control.

By the last quarter of the twentieth century, extensive systems of mass surveillance had been established throughout all liberal capitalist societies, each of which depended on the documentary identification of individuals. In the late 1970s, for example, James Rule and others examined the uses of six of the most widely held personal documents in the United States: birth certificates, driver's licenses, social security cards, passports, bank books, and credit cards.[12] These documents provided vital links between the individuals holding them and the organizations issuing them. Just how document-dependent individuals become is dramatized when

[9] Goffman 1956.
[10] Abercrombie, Hill, and Turner 1986: 33.
[11] Ibid.: 189.
[12] Rule, McAdam, Stearns, and Uglow 1983.

something goes wrong. We all know how awkward and inconvenient it is when one of them is lost or destroyed. From the organizational viewpoint, certainty is given grounds, when dealing with large numbers of otherwise anonymous individuals. Which motorist can renew a license, and which is wanted for violations? Which welfare claimant is a genuine case, and which is double-dipping? Which consumer can purchase this appliance, and which is liable for outstanding debt? The documents will tell.

Rule and his associates noted a trend occurring in the 1970s: the move from self-identification to direct checking. Birth certificates, the production of which is a routine requirement for other documents, are easily obtained by fraudulent means. Yet they still retain some aura of credibility despite their lack of solid warrant. Where credibility is felt to be lacking, however, organizations could increasingly resort to direct checking. Rule found that independent outside sources such as credit bureaus would be used for credit card applications, police records and driver registries for driver's licenses, or immigration databases to check passport presentation at borders. Rule and associates concluded that "[t]he perfection of direct checking within and among organizations is the wave of the future in mass surveillance,"[13] and so it turned out. Increased computerization made direct checking easier and more efficient, even though individual agents are often still warned at some stage that they should not provide false information.

By the 1990s it became clear that so-called information societies were from another point of view surveillance societies, such was the pervasive degree of routine monitoring of almost all aspects of daily life. Surveillance—as focused attention to life details—influences populations in all such societies, although the strength of influence differs according to social factors. The black single mother in the American inner city will find her life much more closely and punitively scrutinized than her counterpart who is an affluent divorcee in the suburbs. The computer-assisted aspect of this, which Roger Clarke calls "dataveillance," had become a taken-for-granted aspect of modern life as new configurations of computing with telecommunications capacities became available.[14] Cross-checking is made simpler through dispersed and networked computer systems. With a range of personal data systems, remote from each other but connected electronically, and a consistent mode of identification, dataveillance can flourish, "feeding on itself," as Rule would say.

However, dataveillance did not proliferate just because new technologies became available. As Colin Bennett notes, these practices were "especially eagerly embraced by governments with neo-conservative

[13] Ibid.: 233.
[14] Clarke 1988.

agendas."[15] Arguably, it is just such choices, emerging from the new political economy of the 1990s, that lay behind the development of the technologies, including their much hyped "convergence."[16] While Manuel Castells' shorthand "information age" may sum up neatly some key characteristics of contemporary societies, it is, as he insists, the implication of new technologies within the current restructuring of capitalism that gives that age its unique dynamic.[17] They permit a new level of networking, particularly of financial flows, and they also make possible the globalization of capitalism. But the same restructuring also demands greater attention to detail, as competition, and awareness of risk, grows. Such details include knowledge of production processes and of consumption, which are gleaned through surveillance.

A key aspect of this restructuring is risk management, a mode of operation that finds echoes in several surveillance sectors. Generalizing from police work, for example, Richard Ericson and Kevin Haggerty claim that "institutionalized risk communication systems form the foundation of contemporary society and provide the governing basis of social life."[18] Within neo-liberal market societies, they suggest, police form just one agency that collects and classifies personal data on behalf of other institutions. But while the knowledge sought may in a sense be personal, it is really only individual, and relates to risk at that. That is, the knowledge is inevitably abstracted from the flesh-and-blood person who relates to others.[19] And in order more exactly to determine the nature and extent of risk, more and more precise knowledge is sought. To decide questions of eligibility, or even of guilt, the risk profile becomes crucially important. And in order to work properly, for most purposes it must also be attached to an accurate identity.

It is thus risk management practices within restructuring capitalist societies that generate the quest for more foolproof, and fraudproof, methods of establishing identity. And this is how the body is brought back in. Once it was merely the existence of unique bodies that was part of the rationale for individuation, and for stabilizing difference. But now, for example, through fingerprinting, other signs of bodily distinctiveness are appealed to. Direct checking from the 1970s on became a matter of verification by a third-party organization. This was done digitally by methods such as data matching once dataveillance regimes were electronically established in the 1980s. But from the 1990s, it became clear that direct checking

[15] Bennett 1996: 237.

[16] This is argued in a related context in Lyon 1988: ch. 2. See also Winseck 1998.

[17] Castells 1996.

[18] Ericson and Haggerty 1997: 426–27.

[19] This distinction between persons and individuals is similar to that appearing in the work of James 1996: xii, 170–71.

would take on yet another meaning: access to tissues, fluids, images, and patterns available from the body itself. Just as direct checking across agencies avoided confrontation with the embodied agent, so direct checking of data produced from within bodies also requires no access to the speech or the memory of the person. It is, once again, abstracted from the person.

Body Surveillance Technologies

To gain entry to a secure or sensitive place one conventionally has to use a password to prove identity and eligibility. Some coded message, memorized by the intending entrant, is repeated at the threshold, before entry is permitted. In the later twentieth century, magnetic stripes and barcoded cards were commonly used for such purposes, whether to enter the laboratory, the prison, or the bank vault. The emergence of body surveillance technologies, however, dispenses with cryptic words and numeric codes. Some part of the physical body—eye, hand, finger, face, voice—is presented to the verification machine. Another level of coding, beyond words and numbers, and relying neither on memory nor on the need to produce a card, turns the body into a password.[20] Apart from the ways in which this may (re)constitute the body as a text, it is a reminder of how access and inclusion, and the distribution of entitlements or powers, may now depend on the display of some body feature.

The machine that confirms identities is usually some form of computerized scanner, which checks the biological feature against the digital file that contains exactly the same characteristics. Thus inmates in Cook County, Illinois, submit to retinal scanning every time they go from jail to court and back; welfare recipients in Connecticut and Pennsylvania have their identities matched to their records by finger imaging; and frequent travelers from Montana to Canada may use an automated voice verification system run by the U.S. Immigration and Naturalization Service to cross the border. According to Davis, in 1997 there were already over ten thousand locations in the United States, from bank vaults to blood banks, where one had to present a body part to go through a door or gain access to a file.[21] Although commercial sources exaggerate the significance of each new product, biometric measures are not merely science fiction. Enough evidence exists to indicate that these modes of identification are becoming increasingly important.

Of course, the use of body parts or processes for identification and surveillance purposes is not new. Fingerprinting has been carried out rou-

[20] See Davis 1997.

[21] Ibid.: 132.

tinely for many decades, as has the use of polygraphs or "lie detectors," which were first used in the United States in the 1930s. As Steven Nock argues, such techniques come in a long tradition of "ordeals" that are meted out to establish or maintain reputations.[22] However, these body surveillance technologies are very limited in scope and they are not always acceptable, for instance, in a court of law.[23] They are used, typically, in cases where suspicion about activities or doubt about identity already exists. They relate to a concept of justice that relies on testimony and evidence to determine individual guilt, not one that routinely places whole populations under "categorical suspicion."[24] Body surveillance is consistent with the emergence of a behavioral approach that cares more about prevention than causes of certain behaviors or social conditions that may help give rise to them.[25]

A consistent feature of contemporary body surveillance technologies is their computer-dependence. In the United States, for example, the FBI began in 1990 to convert its 40 million fingerprint cards and crime history records into digitized records, as part of its ongoing computerization program.[26] As computer power grows, so more applications, previously beyond the reach of automation, become possible. It makes sense, from the point of view of surveillance studies at least, to consider certain biotechnologies as information technologies.[27] This is partly because computerization provides a common digital language for generating, storing, retrieving, processing, and transmitting data from different technological fields, especially in this case, from biotechnology. But more profoundly, when it comes to genetic information, the connections come even closer. Decoding, manipulation, and reprogramming are central to genetic sciences. The Human Genome Project, to take the most significant example, is committed to nothing less than the creation of a vast genetic database that determines the location and chemical sequence of all genes. It has huge surveillance implications.

For instance, some "genomics" companies see their task as using genetic information to increase the production of certain drugs. Others, however, such as Incyte Pharmaceuticals in Palo Alto, California, or Celera, in Rockville, Maryland, sell only data that others use to identify potential drug targets—persons, in other words—depending for their predictions on massive computer power. Along with other agencies that have become more concerned with anticipation and preemption, enabled by new surveillance technologies, the emergent health care paradigm moves steadily from detect-and-treat to predict-and-prevent, with specific therapies aimed at the causes of disease.[28]

Through mapping human genes, detailed information may be obtained about biologically determined features of individuals.[29] The biosurveillance made possible by this relates to the likely course of physical and psychological development of individuals. Such scientific foreknowledge of potential life courses is thus of great interest, especially to employers and insurance companies, who wish to use such data as a means of discrimination between candidates or clients, based on genetic testing and screening. As we shall see, the combination of rising employer health insurance costs and the increasing reliability of genetic testing is likely to encourage the development of such biosurveillance on the large scale. Once again, the body becomes the password, with which (genetic) code entry or exclusion may have very serious social as well as personal consequences.

The drive for perfect knowledge, which includes information about future developments and not merely about past histories, is fostered by risk management discourses, which are in turn the stuff of which insurance companies are made. Restructuring capitalism, and the technological facilitation of fusion among different kinds of information, permits surveillance to move beyond paper files and digitized documents and to infiltrate the body itself. The body, in turn, is treated like a text. It becomes a pass*word*, providing a document for decoding. But texts are best understood in contexts. To illustrate this, we will examine body surveillance as it appears across the whole range of surveillance sectors.

Body Surveillance in Different Sectors

Body surveillance may be found in all social sectors. Two things should be noted about this. The first is that the very notion of sectors sounds rather watertight, when in fact they are increasingly porous. Deregulation and networking means that surveillance data leaks with greater ease from one sector to another, making it less discrete. Nonetheless, the sectors may still be considered to be existing at different points along a spectrum

[22] Nock 1993: 76.

[23] The polygraph is not admissible in Canadian courts, although police may use it to sort out suspicions of criminality. See Ericson and Haggerty 1997: 247. The polygraph is also unacceptable to the American Psychological Association because it turns up "an unacceptable number of false positives"; cited by Marx 1988: 229.

[24] The term is Gary Marx's. See Marx 1988: 219.

[25] Crang 1996.

[26] *New York Times* 1998.

[27] Castells 1996: 30 considers biological and genetic sciences within the "information revolution."

[28] See *The Sunday (Straits) Times* 1999: 42–43.

[29] Regan 1995: 170.

from more to less coercive power. Categorical suspicion may classify subjects at the sharp end of, say, policing, while categorical seduction is more likely to operate at the other, corporate, end. The second point is that by examining the ways in which biometrics are actually used in each sector, some dangers of technological determinism may be avoided. The tendency of studies that focus on the technological is to accept the hype produced by designers and manufacturers, which exaggerates both the use and the usefulness of novel techniques. The fact that some companies are testing biometrics that use body odor today[30] does not mean that we will be passing through smell scanners tomorrow. A survey of the current surveillance uses of biometrics shows that the humble fingerprint, now digitally scanned and stored, is still the technique of choice, although in the workplace genetic screening and testing is gaining ground.

During 1997, the Canadian province of Ontario started to follow the lead of states south of the border in easing the way for increased government use of biometric technologies. The Social Assistance Act was reformed to allow municipalities and the province to identify welfare recipients using biometric data. The aim was to ensure that applicants are only registered once, that when they claim, their identity can be authenticated, and also to permit applicants, recipients, spouses, and adult dependents to gain access to their records.[31] It was estimated at the time that Metropolitan Toronto could save $4.5 million a year in reduced welfare caseloads, and a further $2.7 million in reduced check processing and other administrative expenses.[32] Of course, a neo-conservative agenda is also visible here, one that desires to demonstrate that it has no time for the feckless or the fraudulent. The provincial premier, Mike Harris, expressed his hope that schemes would be established to consolidate health cards, driver's licenses, and other government identification on one card, based on finger-scanning technology.

Such scanners, rather like supermarket checkouts, have glass plates on which the finger is placed. A high-resolution optical image is caught by a camera, and is then converted into a template containing a mathematical equation. For user verification or identification, the system takes a live scan of the fingerprint, comparing it with the stored template. As long as the finger scan is encrypted in different ways for different uses—say, drivers' records and health records—the same scan may be used for different purposes, without the danger of records being shared between agencies. Such reassurances do not always satisfy those closest to welfare recipients, who argue that fingerprinting of any sort is too reminiscent of the

[30] See Davis 1997.
[31] Gage 1997: 32.
[32] Ross 1997: A1, A7.

way that criminals are treated. A further concern is that if biometric methods become universally popular, then the only way of ensuring that they are carried at all times will be to install a chip under the skin of the individual.[33] Because of the already proven use of fingerprinting for law enforcement, and because of the high cost and potential inaccuracies still experienced with some other methods—such as retinal scans or face-recognition—fingerprinting is likely to be seen as one of the best biometric options available.

It cannot be denied that many if not most biosurveillance methods develop from policing and security sectors, which is why when government administration or commercial organizations such as Mastercard propose the use of fingerprint scanning, they have to deal with the question of stigma. The FBI spent $640 million on its "Afis" (automated fingerprint identification system), which was completed in 1999, with 43 million records.[34] But some countries are quicker to adopt biometrics than others, and some techniques catch on in one country but not another. Higher levels of concern about security, and greater fear of crime, may help to account for the faster take-up rate of digitized fingerprinting in the United States than, say, in Canada.[35] Equally, the more intensive use of video surveillance via closed circuit TV in the United Kingdom may explain why face-recognition technologies are being developed more rapidly there than in some other countries.

So while banks such as Citicorp may test face-recognition technologies,[36] their development is more likely to take place in law enforcement contexts. Britain, where photographic technologies have been added to the more familiar convergence between computing and telecommunications, is the world leader in this field. The British Home Office, Police Foundation, and Marks and Spencer's have joined forces to produce reliable automatic visual recognition of suspects.[37] Limited systems are already in use, such as the "Football Intelligence System" in Greater Manchester. Information and photographic records of suspects and offenders associated with soccer violence is collated such that pictures of "likely suspects" can be drawn from the database. The equivalent National Criminal Intelligence Service database used photophones to transmit digitized photographs of suspected hooligans to participating football grounds in the 1996 European championship. Similar systems are being developed for use at Sydney International Airport in Australia.[38]

[33] Clarke 1997.
[34] Cottrill 1997: 11.
[35] Keenan, cited in Gage 1997: 32.
[36] Davis 1997.
[37] Norris et al. 1996: 265.
[38] Ibid.: 267.

Other techniques that cross the border from policing and law enforcement to the economic private sector include genetic testing. The use of DNA samples from suspected rapists and murderers is well known, and has led to a number of convictions and retrials. Evidence of criminal activity or involvement may be obtained from DNA samples in plucked hair, blood, and saliva that match each unique individual. The American CODIS ("Combined DNA Index System") is a national DNA identification system. Fifteen or more states are now using collected samples to add to the CODIS databank. In Canada and the United Kingdom, too, such samples may be collected without consent, as DNA profiling becomes routine.[39] Whatever might be said about the diminution of due process in such cases, the fact remains that DNA testing by police is relatively uncontroversial. The same may not be said for genetic tests and screens in the workplace.

Employers, wishing to minimize risk, may use genetic screening to determine susceptibility to disease, such as breast, ovarian, colon, thyroid, eye, kidney, and skin cancers, or Huntington's Disease, among employees, or to check levels of damage from exposure to hazardous materials at work. But genetic discrimination could result on the basis of such tests. At the same time, fear of such discrimination could discourage some people from undergoing tests from which they might benefit. This points up, once more, the all-too-frequently forgotten fact that surveillance has two faces. The same genetic test, in this case, may be the means of personal benefit, say, enabling the person to seek treatment for a medical condition before it is too advanced, and of personal discrimination, blocking the path to promotion or retention.

It should be remembered that the desire to control the workforce is far from new, and that concerns with aspects of the body and its condition are not new either. But during the twentieth century technical and bureaucratic types of control became less effective, which is one reason for the turn toward "personal control." An additional reason is the perceived failure of socializing institutions such as family and school. What is new is to see the workplace as the locus for social control over personality and health, via pre-hire screening, drug testing, polygraph testing, stress management, wellness programs, AIDS testing, and programs for alcoholism, weight reduction, and gambling addiction.[40] This is the background to the use of DNA evidence in workplace body tests, and also represents a blurring of the boundary between state-sponsored and private forms of social control. In many cases, such as urinalysis for drug testing, part of the purpose is indeed to produce the "perfect worker," but another part

[39] Ericson and Haggerty 1997: 248. See also Pamela Sankar's essay in the present volume.
[40] Wagner 1987: 540–41.

is to make a symbolic moral gesture to the public as to where true standards are to be found.[41]

Controversy breaks out when genetic testing starts to be used as a condition of employment, and it is against such discrimination that legal protection has been sought in the United States and elsewhere. In the late 1990s Lawrence Berkeley National Laboratory in California was successfully sued by seven employees who learned that blood and urine obtained during preemployment medical examinations had been tested for syphilis, sickle cell anemia (black applicants), and pregnancy (female applicants). The appeals court ruled that such tests required the consent of the employee, or that they have a direct bearing on one's ability to do the job.[42] Further controversy surrounds the accuracy of genetic testing. After all, genes alone do not determine an individual's future health. Diet, exercise, psychosocial factors, and economic class may affect an individual's health almost as much as genetics.[43]

If in the workplace the capitalist corporation intensifies its body surveillance in an attempt to perfect the worker, in the marketplace the consumer is increasingly subject to biometrics, a process that is stimulated particularly by the projected growth of electronic commerce. While the potential for electronic commerce has been clear for some time, the relative lack of security—especially of identification—has proved a major deterrent for some. But not only burgeoning electronic commerce is behind the quest for biometric identifiers. Risk management in general lies behind many attempts to ensure biometrically that identification of clients and customers is as accurate and as efficient as possible.

While fingerprint-based biometrics are, understandably, still prevalent in government administration and policing, the situation is much more volatile in the private sector. Here, fingerprint biometrics are not unknown—MasterCard is moving to such a system to combat credit card fraud[44]—but other methods are more widespread. While genetic profiling and screening is perhaps the fastest growing—and the most controversial—form of body surveillance in the workplace, in its present state of development it is unlikely to become popular in the marketplace. In the commercial, consumer sector, a range of biometrics is vying for preeminence, and none is yet a clear winner. Indeed, competition will probably ensure that this situation will continue for some time, at least until some

[41] Boyes-Watson 1997. See also Hartwell, Steele, French, and Rodman 1996, who argue that it is drug abuse rather than the larger employment problem, alcohol abuse, for which employees are more frequently tested (two times as much, in fact) in the United States. Alcohol use is not in itself illegal or against company policies.
[42] Mineham 1998: 208.
[43] Smith 1998: 38.
[44] Surtees 1996: B4.

Other techniques that cross the border from policing and law enforcement to the economic private sector include genetic testing. The use of DNA samples from suspected rapists and murderers is well known, and has led to a number of convictions and retrials. Evidence of criminal activity or involvement may be obtained from DNA samples in plucked hair, blood, and saliva that match each unique individual. The American CODIS ("Combined DNA Index System") is a national DNA identification system. Fifteen or more states are now using collected samples to add to the CODIS databank. In Canada and the United Kingdom, too, such samples may be collected without consent, as DNA profiling becomes routine.[39] Whatever might be said about the diminution of due process in such cases, the fact remains that DNA testing by police is relatively uncontroversial. The same may not be said for genetic tests and screens in the workplace.

Employers, wishing to minimize risk, may use genetic screening to determine susceptibility to disease, such as breast, ovarian, colon, thyroid, eye, kidney, and skin cancers, or Huntington's Disease, among employees, or to check levels of damage from exposure to hazardous materials at work. But genetic discrimination could result on the basis of such tests. At the same time, fear of such discrimination could discourage some people from undergoing tests from which they might benefit. This points up, once more, the all-too-frequently forgotten fact that surveillance has two faces. The same genetic test, in this case, may be the means of personal benefit, say, enabling the person to seek treatment for a medical condition before it is too advanced, and of personal discrimination, blocking the path to promotion or retention.

It should be remembered that the desire to control the workforce is far from new, and that concerns with aspects of the body and its condition are not new either. But during the twentieth century technical and bureaucratic types of control became less effective, which is one reason for the turn toward "personal control." An additional reason is the perceived failure of socializing institutions such as family and school. What is new is to see the workplace as the locus for social control over personality and health, via pre-hire screening, drug testing, polygraph testing, stress management, wellness programs, AIDS testing, and programs for alcoholism, weight reduction, and gambling addiction.[40] This is the background to the use of DNA evidence in workplace body tests, and also represents a blurring of the boundary between state-sponsored and private forms of social control. In many cases, such as urinalysis for drug testing, part of the purpose is indeed to produce the "perfect worker," but another part

[39] Ericson and Haggerty 1997: 248. See also Pamela Sankar's essay in the present volume.
[40] Wagner 1987: 540–41.

is to make a symbolic moral gesture to the public as to where true standards are to be found.[41]

Controversy breaks out when genetic testing starts to be used as a condition of employment, and it is against such discrimination that legal protection has been sought in the United States and elsewhere. In the late 1990s Lawrence Berkeley National Laboratory in California was successfully sued by seven employees who learned that blood and urine obtained during preemployment medical examinations had been tested for syphilis, sickle cell anemia (black applicants), and pregnancy (female applicants). The appeals court ruled that such tests required the consent of the employee, or that they have a direct bearing on one's ability to do the job.[42] Further controversy surrounds the accuracy of genetic testing. After all, genes alone do not determine an individual's future health. Diet, exercise, psychosocial factors, and economic class may affect an individual's health almost as much as genetics.[43]

If in the workplace the capitalist corporation intensifies its body surveillance in an attempt to perfect the worker, in the marketplace the consumer is increasingly subject to biometrics, a process that is stimulated particularly by the projected growth of electronic commerce. While the potential for electronic commerce has been clear for some time, the relative lack of security—especially of identification—has proved a major deterrent for some. But not only burgeoning electronic commerce is behind the quest for biometric identifiers. Risk management in general lies behind many attempts to ensure biometrically that identification of clients and customers is as accurate and as efficient as possible.

While fingerprint-based biometrics are, understandably, still prevalent in government administration and policing, the situation is much more volatile in the private sector. Here, fingerprint biometrics are not unknown—MasterCard is moving to such a system to combat credit card fraud[44]—but other methods are more widespread. While genetic profiling and screening is perhaps the fastest growing—and the most controversial—form of body surveillance in the workplace, in its present state of development it is unlikely to become popular in the marketplace. In the commercial, consumer sector, a range of biometrics is vying for preeminence, and none is yet a clear winner. Indeed, competition will probably ensure that this situation will continue for some time, at least until some

[41] Boyes-Watson 1997. See also Hartwell, Steele, French, and Rodman 1996, who argue that it is drug abuse rather than the larger employment problem, alcohol abuse, for which employees are more frequently tested (two times as much, in fact) in the United States. Alcohol use is not in itself illegal or against company policies.
[42] Mineham 1998: 208.
[43] Smith 1998: 38.
[44] Surtees 1996: B4.

standards have been established. The first commercial biometric, a hand scanner used in a Wall Street firm to monitor employee attendance, was introduced in 1974,[45] but it was only in the 1990s that the techniques improved and the prices fell sufficiently to make them commercially viable. Lotus employees pass through a hand scanner to pick up their children from day care, and Coca Cola uses them to ensure that only identified employees punch their time cards.[46]

The most widely used commercial biometric is the handkey,[47] which is in use for frequent travelers in New York and Toronto airports, at immigration desks, and was the means of controlling access of 65,000 atheletes and their teams to the Olympic Village in Atlanta in 1996. Despite some negative responses to them, biometrics based on fingerprints are also in use commercially, including the so-called biomouse, used for securing access to computers. Single fingers, or all fingers and thumbs, can be scanned in, scrambled, reduced, and stored, ready for use each time the authorized person wishes to use the machine. Systems such as this are likely to prove popular because they can also be used for remote log-in, ID card validation, electronic signature, and financial transaction authorization.[48]

The eye is another key body part suitable for biometrics. Although retinal scans are the most accurate identifiers, because of their expense and their slightly awkward use they tend to be favored mainly by governments. The CIA, for instance, uses retinal scanners, along with voiceprints, in its top security computer vault in Langley, Virginia. The person has to lean over and place his or her face on a bar close to the machine, which passes a red light beam across the eye. Iris scans, on the other hand, are favored for automated bank machines, partly because they dispense with positioning devices and beams. As the customer approaches, video cameras zoom in to identify the form as a person, then to fix the person's coordinates. From a meter away, an eye image is taken, to be matched—in two or three seconds—with the digitally encoded iris image on file.[49] OKI Electric Industry, Japan, and NCR Knowledge Lab in London, United Kingdom, are among those testing iris scanning devices.

Body Surveillance: Movement, Action, and Risk

The body has become not only a site of surveillance, but a source of surveillance data. The practice of locating, tracking, and controlling bodies

[45] Beiser 1997: 40.
[46] Davis 1997: 132.
[47] Beiser 1997: 40.
[48] Guly 1997: 23.
[49] Powell 1997: E1, E11.

is as old as history, although it was routinized and intensified by the disciplines of modernity. The idea of checking identities by reference to unique features, above all faces, is equally ancient, although only in modern times have distinguishing characteristics such as fingerprints become important for verifying identity. Today, both aspects of body surveillance are becoming increasingly significant at the same time, which suggests that they may be related. Looking at movement, action, and risk shows how.

First, modern societies are marked by mobility, which means that bodies are on the move. Today's transportation enables people to travel, by transit systems across the city and by airline systems around the world. People travel for work and for pleasure, in the tourist delights of the rich and in the tragic displacements of refugees. Mobility means different things to people in different social groups. Travel is experienced differently by the urban commuter in his air-conditioned car on the freeway than by the low-wage earner who waits in the rain for a crowded bus to get to work. Such mobility also means that we tend to interact more and more with strangers, people with whom we have no real relationship, who do not know who we are or if they can trust us. So symbols of the stable self, such as driver's licenses, credit cards, passports, or identity papers, have to be presented to prove ourselves. The society of strangers requires tokens of trust.[50]

Each token of trust, however, now connects with others in a web of identification and credential surveillance systems. Such systems serve to keep tabs on those moving bodies and to ensure that only authorized bodies enter certain rooms, cross certain borders, claim certain benefits, or travel on certain highways or airlines. They are a means of social control, social orchestration, and social influence. But actual moving bodies are not the only things to be caught in the electronic eye. An increasing proportion of significant interaction today is bodyless, mediated above all by electronic means. And this is how the two kinds of body surveillance come to be connected.

The more other means of mediating social relationships appear, the more the signs of surveillance appear with them as well. What worked to coordinate and control bodies in conventional time and space can be transposed into the virtual world of cyberspace. This newer sphere of transactions, and thus of flows of information and power, is now a further site of surveillance. As Paul Virilio says, here "people can't be separated by physical obstacles or by temporal distances. With the interfacing of computer terminals and video-monitors, distinctions of *here* and *there* no longer mean anything."[51] But it is precisely in those channels that carry

[50] Giddens 1990.
[51] Virilio 1991: 13.

the flows of information that precision is increasingly required. They are too porous for cyberspace to be secure, hence the quest of PETs and of body surveillance to keep identities intact.

Second, consider the category of action. By this, I refer back to my introductory comments on personal identity as being a matter of recognizing a unique body, of gaining access to memory, and of according responsibilities and rights to the person. Body surveillance reduces identity questions to what can be found in the text of the body itself. It bypasses the acting subject, who may wish to explain herself, or to put things in a longer historical context, by appealing only to the speechless "truth" that DNA samples or handscans can provide. It is data from the object of the body rather than speech from the acting subject that is to be relied on in the last analysis. Good reasons for using body surveillance may be produced, showing that criminals may more easily be apprehended or that fraud may be reduced in commerce, but body surveillance should also be viewed as part of wider social trends.

Ontario's information and privacy commissioner, Ann Cavoukian, is an advocate of biometric encryption for secure identification, for instance, in health information networks. She points to the paradox that biometrics is a sinister surveillance threat if it is identifiable, but when encrypted becomes a "protector of privacy."[52] Thus the interests of both individuals and organizations are served. Individuals can keep their privacy through the anonymity of encryption, and organizations can be assured of the authenticity of individuals they conduct business with. Few would wish to quarrel with this argument. It does not mean, however, that organizations are any less distrustful of individuals they deal with, or that such individuals are any less concerned to guard their privacy. It is, after all, because of the quest for privacy within the society of strangers that tokens of trust are required in the first place.

The choice to take surveillance through the threshold of the skin and inside the physical body may raise privacy questions—are our truly private parts now within the body rather than on its surface?—but it also has to be seen in the context of a new behaviorism that treats the body as authoritative text. In the quest for more knowledge to combat risk, body surveillance appears as a worthy source. It promises to offer not only detail of what has happened in the past—how many times previously this person has entered this building or has made that transaction—but also of what will happen in the future. Risk discourses are especially concerned with knowledge of the future. As Ulrich Beck says, the "centre of risk consciousness lies not in the present but in the future."[53] Thus body

[52] Cavoukian 1999: 117.
[53] Beck 1992: 34.

surveillance, above all that which uses DNA, appears as the natural next wave. This is not merely the perfect match, sought so assiduously by those obsessed with identification, but the dynamic match, that holds histories and simulated futures for comparison and checking.

The result is that body surveillance takes its place as part of a more general transformation of the ways social activities and human agency are understood. In the workplace, it is no longer merely one's qualifications, aptitude for the job, or personal bearing at interview that counts. A fifty-three-year-old man being interviewed for a job with an insurance company revealed that he has hemochromatosis but was asymptomatic. At the second interview he was told he might be hired, but with no insurance plan. He agreed to this but at the third interview was told that he could not be hired because of his genetic condition.[54] One's potential future health condition is now grounds for job discrimination, segregation, and classification. In policing, too, the future is in focus. As Ericson shows, "Risk communication systems turn the moral discourse of deviance into a utilitarian morality of probability calculus. . . . Gutted of moral wrongdoing, deviance is treated as a normal accident . . . a contingency for which there are risk technologies to spread the loss and to prevent recurrence."[55] Body surveillance, bound up with identities and identification provided by police, signals another moment in the shift toward actuarial justice.

Risk and security may appear to be highly important to social well-being. This is especially so in societies that tend to minimize the signficance of the past, and are prepared to rely on imagined futures, simulations, to guide practices and policy in the present. If the primary documentary identification is the human body itself, then this is bound to sit uneasily with views of identity that go beyond what can be learned from a bodily ordeal or the testing of tissue and fluid. Autobiography and the social web of identities are diminished if not discounted in such body surveillance identification regimes. Beyond this, too, one must ask what is the likely next stage. And one may ask this, not as another exercise in social science fiction, but as a way of following current technologics. If it becomes common to have to present a chip—in a smart card—bearing a biometric identifier, then the requirement to carry this chip at all times will become strong. The only way to guarantee this would be, as Roger Clarke says, to "mount it in the carrier," that is, "to install it in the person's body."[56]

Third, such a scenario raises further questions. These are not just questions of moving bodies and bodyless transactions, coordinated in time and space, or of the paradoxes of the private and of human action, when

[54] National Genome Project Research Institute 1998: 3.
[55] Ericson and Haggerty 1997: 448.
[56] Clarke 1997: 2.

identification is reduced to direct access to the body. The further questions concern relations between technology and society in general. For surveillance attempts constantly to upgrade the knowledge it obtains for risk management, in the belief that the more advanced the technoscience instrument, the more accurate the knowledge. In the case of body surveillance and identification, precision is the aim. But what do the "advances" entail? On the one hand, as I have shown, a new mode of justice emerges to keep in step with the focus on the future and on risk. On the other, the possibility is mooted of body modification in the interests of infallible identification. Are these the prices that must be paid for "advance"?

One obvious question concerns the reliability of the new body surveillance technologies. As noted above, the most reliable identifiers are also the most expensive. Digital fingerprinting, which builds on older technologies, tends to be used for administration purposes, particularly welfare. But fingerprinting can exclude otherwise eligible persons who may have skin diseases. A case in point is Kenneth Payne, a Los Angeles man who qualified as a teacher in his forties. He cannot obtain employment because he suffers from atopic dermatitis, which makes his skin blister and peel, thus spoiling his fingerprint. For security reasons California requires all teachers to pass a fingerprint test. No print, no job.[57] The much more accurate retinal scan is restricted due to its price. Understandably, people also feel protective of their eyes and are concerned about light beams passing across them. Voiceprints and facial scanning have yet to find widespread use, and there are questions about accuracy. Faces may change considerably at different times of the day, and a voice may alter when someone has a cold.[58]

Similarly with the use of DNA, accuracy is not guaranteed by any means. Moreover, employers may use genetic information in different ways, depending on the situation. When testing applicants for jobs, it may be assumed that the genetic predisposition alone is enough to disqualify someone—this despite what is known about other factors, such as environment, that will affect an individual's susceptibility to disease. If, on the other hand, screening for the effects of toxic materials is in question, employers have been known to bring the "other factors" into play. "They tend to give the benefit of the doubt to the chemicals" and to "hold the outside environment or people's lifestyle choices responsible for worker disease."[59] And as with biometrics, it must be acknowledged that the body itself may be incapable of yielding the secrets for which it is infiltrated. None of us has perfect genes.

[57] Reed 1998.
[58] Gage 1997: 32.
[59] Draper 1997: 11.

Huge potential dangers are raised of biometric data circulating among databases and being traded among companies. These hazards lie behind the pressure for encryption and for one-to-one—smart card—matching systems. When identification is required, the biometric reader would simply match the particular body part with the data on the card.[60] The person holding the card would retain control, or at least that is the theory. It is particularly when the next step, chip implants, is proposed, that other surveillance specters raise their heads. Civil libertarians balk at this, and in so doing find themselves in the unfamiliar company of religious fundamentalists. In 1995, for instance, American televangelist Pat Robertson hosted a segment called "Biometrics: Chipping Away Your Rights." He declared that "The Bible says that the time is going to come that you cannot buy or sell except with a mark placed on your hand or on your forehead."[61] The so-called mark of the beast appears to have arrived with biometrics and genetic IDs.

It is interesting that this implant has such negative connotations among civil libertarians and fundamentalists. This is the other side of the coin, it seems, from the cyborg as a liberator, that allows for playful transgressions of old boundaries and the political potential to revise categories such as gender.[62] Sadie Plant, for instance, examines ways, not of altering the body, but of transcending it technologically so that bodies can be represented more flexibly.[63] But such flexible representation stands in rather stark contrast with the desire directly to tap into the body to obtain information untainted by the subject. This latter cyborg, it seems, is stripped of consciousness and the capacity to answer for herself, all in the paradoxical interests of accurate identification. In order to work, the old disciplinary technologies that attempted to direct the body still relied on ideas such as reflexivity, self-consciousness, even conscience. Newer regimes of risk, surveillance, and security require less and less that the subject be—literally—response-able.

Body Surveillance, Identification, and Identity

To connect the biblical book of Revelation directly with biometrics is a typically literalistic ploy of fundamentalism. It tends to produce cynically dismissive responses, which could, ironically, fuel the very complacency that the more apocalyptic doomwatchers wish to combat. A non-literalist

[60] Davis 1997: 6.
[61] Cited in ibid.: 4.
[62] See, for example, Haraway 1997.
[63] Plant 1995.

reading of the same text, however, is salutory. This ancient book, which warns of things to come and promises hope for the faithful, is surprisingly appropriate in its assessments of power and knowledge. The beast whose mark is inscribed in the bodies of would-be buyers and sellers is a "beast from the earth,"[64] the symbol of a kind of false faith or, as Michael Wilcock suggests, an ideology.[65]

By this interpretation neither the technology nor the social entity need be identified precisely. But the relevance of the idea of the beast's mark to any kind of identifiers, including biometrics, becomes both more plain and more plausible. Simulated surveillance, which attempts to bring imagined futures to bear on the practices of the present, depends upon a dream of perfect knowledge.[66] This dream has ideological power to breathe life into the polycentric webs of the contemporary network society. The mystical mark confirms those in the thrall of the system. But the dream is a deceit, no less than was Jeremy Bentham's when he first projected the Panopticon as secular omniscience.[67]

In the steady shift from identification papers to body surveillance, reliance on data images rather than persons-with-distinctive-identities is further strengthened. Risk management, obsessed with accurate information, now sends its surveillance probes under the skin. New technologies are rapidly being developed, harnessed, and—importantly—recombined, to pursue these ends. Whether or not implants become a widespread reality,[68] the resulting involuntary cyborg will be increasingly dependent on technologically encoded body data for access and eligibility to the mundane functions of everyday life. Given this reality, urgent questions are raised about the means, political, educational, and, yes, technological—such as encrypted biometrics—of limiting the potential damage that such deepened dependence on the data image could cause.

[64] Revelation 13: 16–17.

[65] Wilcock 1975: 127.

[66] This is a key theme of Bogard 1996. One need not accept all aspects of his "social science fiction" to see that this present point is well made by him.

[67] Lyon 1991: 98.

[68] Kevin Warwick at Reading University, United Kingdom, voluntarily implanted a chip under his skin in August 1998, in order more fully to control his surrounding environment. Needless to say the same kind of chip has the potential to be used in ways that monitor and influence the person in which body the chip is mounted.

17

Identity and Anonymity: Some Conceptual Distinctions and Issues for Research

GARY T. MARX

> "You ought to have some papers to show who you are." The police officer advised me.
> "I do not need any paper. I know who I am," I said.
> "Maybe so. Other people are also interested in knowing who you are."
> —B. TRAVEN, *The Death Ship*

THE DOCUMENTATION of individual identity, whether by the state, private organizations, or individuals, can be located within a broader set of questions concerning identity and anonymity.[1] This topic involves the sociology of personal information and of information more generally. These in turn nestle within the wider field of the sociology of knowledge. Current developments in the area of personal identification are a small part of broader changes in contemporary means of information collection, processing, and communication.

My interest in the topic grows out of research on the "new surveillance," which includes technologies such as computer matching and profiling, video cameras, electronic location monitoring, and biometric devices, which have the potential to identify individuals, independent of their will and even knowledge.[2] Developments in biometric identification and smart card technology and debates over national ID cards and privacy are also elements of this.

The extractive power of the new surveillance leads to value and policy questions such as "under what conditions is it right or wrong to collect various kinds of personal information with and without consent?" and "when should individuals be compelled to reveal and when should they have a right to conceal?" While these are normative questions, answers

[1] This essay draws from a book tentatively entitled *Windows Into the Soul: Surveillance and Society in an Age of High Technology* based on the American Sociological Association–Duke University Jensen Lectures.

[2] See, for example, Rule 1973; Foucault 1977; Laudon 1986; Marx 1988; Clarke 1988: 29–45; Gandy 1993; Lyon 1994; Lyon and Zureik 1996; Curry 1998; and Staples 1997.