Genetics, biometrics and the informatization of the body

Irma van der Ploeg
iBMG, Erasmus University MC, Rotterdam and Zuyd University, Heerlen, The Netherlands

Summary. "Genetics" is a term covering a wide set of theories, practices, and technologies, only some of which overlap with the practices and technologies of biometrics. In this paper some current technological developments relating to biometric applications of genetics will be highlighted. Next, the author will elaborate the notion of the informatization of the body, by means of a brief philosophical detour on the dualisms of language and reality, words and things. In the subsequent sections she will then draw out some of the questions relevant to the purposes of Biometrics Identification Technology Ethics (BITE), and discuss the ethical problems associated with the informatization of the body. There are, however some problems and limitations to the currently dominant ethical discourse to deal with all things ethical in relation to information technology in general, and biometrics or genetics in particular. The final section will discuss some of these meta-problems.

Key words: biometrics, genetics, DNA-banking, ethics, informatization of the body, privacy.

Riassunto *(Genetica, biometria e informatizzazione del corpo)*. Genetica è un termine che comprende un gran numero di teorie, pratiche e tecnologie, di cui solo alcune sono comprese tra le pratiche e le tecnologie biometriche. In questo articolo vengono illustrati alcuni sviluppi tecnici connessi alle applicazioni biometriche della genetica. In seguito si elaborano nozioni di informatizzazione del corpo attraverso alcune brevi digressioni filosofiche sul dualismo tra linguaggio e realtà, su parole e cose. In una sezione successiva si affrontano alcune questioni di rilievo per il progetto Biometrics Identification Technology Ethics (BITE) e si discutono i problemi etici associati con l'informatizzazione del corpo. Ci sono, tuttavia, alcune questioni insolute e alcuni limiti nel modo in cui il pensiero etico dominante ha affrontato il rapporto tra etica e tecnologie dell'informazione in generale e, in particolare, quello tra genetica e biometria. Nella sezione si discutono alcuni di questi meta problemi.

Parole chiave: biometria, genetica, banche del DNA, etica, informatizzazione del corpo, privacy.

INTRODUCTION

In a project devoted to biometrics, it may not be all that self-evident to devote a lot of attention to genetics. Genetics is a very special case within the class of biometric technologies; some would even argue that because of its special character it does not even belong in the same class. "Genetics" is a term covering a wide set of theories, practices, and technologies, only some of which overlap with the practices and technologies of biometrics.

On the other hand, genetics can be regarded as the epitomization of a more general development to which all biometric technologies contribute. A development that can be characterized as the *informatization of the body* [1, 2], a relatively new phenomenon in which the human body appears to be redefined as an entity made of information. It is to this phenomenon of the emergence of the body as information that remarks in this chapter about genetics will primarily relate.

First, some current technological developments relating to biometric applications of genetics will be highlighted, which subsequently will be placed in a wider technological context relevant to the central topic. Next, the notion of the informatization of the body will be elaborate by means of a brief philosophical detour on the dualisms of language and reality, words and things.

In the subsequent sections the author will then draw out some of the questions relevant to the purposes of Biometrics Identification Technology Ethics (BITE), and discuss the ethical problems associated with the informatization of the body.

There are, however some problems and limitations to the currently dominant ethical discourse to deal with all things ethical in relation to information technology (IT) in general, and biometrics or genetics in particular. The final section will discuss some of these meta-problems with a short discussion of this discourse, and propose an additional one that may help to overcome some of these problems.

RELEVANT CURRENT DEVELOPMENTS

DNA banking: ever more inclusive databases

The primary use of genetics as biometric identification technology is in forensic identification of

Indirizzo per la corrispondenza (Address for correspondence): Irma van der Ploeg, Zuyd University, P.O. Box 2606, Heerlen,The Netherlands. E-mail: i.vdploeg@hszuyd.nl.

suspects. Evidence based on DNA identification has been accepted as legitimate evidence in many countries, and police organizations have been steadily collecting and storing DNA information of suspects and convicts.

Over the past decennium the trend has been for these databases to become increasingly inclusive. For example, in The Netherlands, the criterion for inclusion in the national police DNA-bank used to be being suspected of a crime with an 8-year sentence. In 2001 this was changed into 4 years, and currently, proposals are being discussed about banking cell material and DNA of every person convicted of crime, and allowing generation of a suspects' profile, determining characteristics of appearance, on the basis of trace DNA. In the UK, the recognised "world leader" in forensic DNA databases, the criteria for inclusion has advanced from those people convicted of a crime, to those charged, and then in 2004, simply to those arrested. On an international level, talks about increasing cooperation in the areas of security, law enforcement, and policing, include the idea of exchanging DNA data. According to a Wellcome Trust research notice, a range of organizations are currently involved in developing and promoting DNA databasing across the EU. For example: the European DNA Profiling Group (EDNAP), has existed since 1988 with the aim of establishing systematic procedures for data-sharing across the European community; the Standardization of DNA Profiling in the European Union (STADNAP) group exists to promote co-operation across the EU in order to utilize DNA profiling to detect "mobile serial offenders"; and the European Network of Forensic Science Institutes (ENFSI) has similar ambitions to standardize forensic practices in support of policing across the whole of the EU. The EU itself provides funds (as, for example, to STADNAP) to ascertain best practices capable of facilitating increased data sharing across criminal jurisdictions [3].

The point is that, for criminal investigation purposes, such databases become more effective the larger and the more inclusive they are. This fact is the reason that, once started, the collection of material from ever larger sections of the population becomes so attractive; the most ardent advocates can be heard to argue that it would make good sense to sample the entire population, for example by routine collection of DNA from every newborn. However, including the entire population actually decreases efficacy of the databases for investigation purposes, since 99% of the enrolled will not engage in criminal behavior anyway, thus only increasing the chances of generation of large numbers of false positives, and increasing the burden of selecting the relevant matches from the irrelevant. In a context of increasing (international) exchange and rendering interoperable of dispersed systems and databases, it is interesting to take note of the existence of large biological sample banks in the medical sector. In the course of various population screening programmes, large numbers of blood, urine samples, cell material etc. is being stored in hospitals and medical research centers all over the world. Potentially, these can provide the material for DNA analysis if ever this might be deemed necessary and legal.

From fingerprinting to profiling

The term DNA-fingerprint, sometimes used instead of DNA typing or identification, refers to the fact that the genetic information used in DNA identification technology did not yield any information about the person involved beyond the matching of identity. For this reason, many privacy and data-protection issues were not deemed relevant with regard to DNA-identification technology. The polymorphisms used in this technology were believed to be non coding for specific traits or predispositions. However, with current technologies, this is no longer the case. The recent UK *Police Science & Technology Strategy 2003-2008*, for instance, asserts the commitment to develop the capacity for "identifying offender characteristics from DNA". The British Forensic Science Service (FSS) has been investigating the possibility of predicting physical characteristics of individuals for some time. They have created a "Red Hair database" which claims to identify "84% of redheads", and they now offer the police an "ethnic inference service" which claims the capacity to discern – with unknown degrees of certainty – ethnic origin from DNA profiles. The FSS are currently researching the identification of a range of other phenotypical traits, such as facial characteristics, height and eye colour. These ambitions are also becoming linked to another important, and quickly expanding, way of ascertaining identifying characteristics from DNA afforded by "haplotype mapping" – for example, in the Y-STR database which is concerned to make an "assessment of male population stratification among European and world-wide populations". All of these technological developments involving the interrogation of the "coding regions" of the human genome raise new policy and ethical issues for those involved in the use of genetic information for crime investigation [3].

From monogenetic causality to multi-factorial probabilities and predispositions

There is a development within the wider domain of medical genetic research countering the risk of unwanted disclosure of genetic information to third parties, often associated with the above. The former optimism within medical genetic research of finding genetic causes for diseases by locating them in specific monogenetic deviations and defects, has been gradually replaced by the more realistic expectation that such discoveries will remain exceptional. Instead, most diseases turn out not to be caused by a single genetic defect, but by a complex set of etiological factors, only a part of which are genetic in nature. Moreover, even if the cause is definitely genetic, usually many genes are involved, that may or may not be located in proximity of each other.

Besides reducing the hope of genetic therapies becoming available, it also decreases the value of genetic profiles as predictors of medical conditions and personal traits. The fears of disclosure of genetic information to third parties, for example employers or insurance companies, were largely based on the possibility of being singled out as a "burning house", thus finding oneself part of a select high risk group, with diminished chances of getting insured or finding employment. As it turns out with the new insights, most of us will prove to be not "burning", but "smoldering houses", which makes the chances and rationality of individual discrimination very limited [4].

Even if the trend is towards getting more and more predictive information from DNA samples, the features now on the research agendas are very general ones, shared by large parts of the population. Although this may be of help in criminal investigations to exclude a specific suspect, the possibilities for gaining significant predictive medical information will, in all probability, remain limited.

CONTEXT OF BROADER TECHNOLOGICAL DEVELOPMENTS

The increased collection and storage of genetic information in electronic form in searchable databases may be considered part of a wider development. Today we are witnessing a proliferation of technologies that are geared towards the generation, collection, processing, and analysis of digital body data. In various domains of society, technologies are put to use that, for various purposes, involve the interfacing of human bodies with machines in order to transform certain physical characteristics into digital data. The set of technologies studied in the BITE project, collectively referred to as biometric identification technologies, clearly fall within this category. Analogous the "machine readable travel documents" or MRTDs with which biometrics have recently become strongly associated, we see biometrics implicated in the co-construction of *machine readable bodies*.

Generally speaking, biometric technology involves the collection with a sensoring device of digital representations of physiological features unique to an individual, like a fingerprint, pattern of the iris, the retina, the veins of *e.g.* the hand, physiognomic features, shape of the hand, or voicepatterns; it may also include typical behavioral patterns like typing or writing a signature. This digital representation of biometric data is then usually transformed via some algorithm to produce a socalled "template". This algorithmic transformation is said to be irreversible, meaning that from the template one cannot deduce the biometric data themselves. These templates are stored in a centralized database that is accessed when on following occasions the finger, hand, face, eye or voice is presented to the system. After a similar algorithmic transformation of this second biometric image, a comparison can be executed. If a matching template is found, the person presenting themselves is "recognized" and counts as "known" to the system. It may also be the case that templates are not stored centrally, but on a chip, inserted into *e.g.* a passport, instead. The user then has to present both chip and requested body part to "prove" they are the legitimate user of the passport. In addition, the healthcare domain is, obviously, deeply involved in that which we refer to as "the informatization of the body". Many of the late twentieth-century advances, both in medical science and in the organization of healthcare delivery, are largely attributable to various applications of information technologies. From admission, through diagnostics, to delivery of therapies and medication, up to payment and reimbursement, a patient's trajectory through the healthcare system today is from beginning to end thoroughly IT mediated. The complexities of advanced forms of cancer therapy, with their complicated protocols for administering precise medication and radiation dosages, for example, would be impossible without redefining at least part of the process in terms of information gathering strategy and data management. And even on a more low-tech level of medical care, such as delivered, for example, in general practice, patient data are painstakenly registered in electronic patient records, collected in national registries, and sent to and fro between medical professional, pharmacists, insurers, policy institutions, etc. – or at least that is being planned for. The result is an incredible amount of detailed and specific electronic data on peoples' (psycho-)somatic and embodied social being in numerous databases.

In the context of discussing genetics and its potential for identification practices, it is also good to remind ourselves once more of the existence of all the tissue, blood, cellmaterial, skin, gamete, and embryo banks. These may not be accurately labeled as electronic databanks with body data such as they are, but potentially, and without clear regulation or legislation [5], a court order might suffice to turn any of these biological samples in as many DNA-profiles.

At first glance, these highly diverse technological practices may seem to have little in common. However, the reason to bring them together like this, is to highlight a commonality that we consider to be of high cultural and ethical significance. Each one of them, in one way or another, involves the transformation of particular aspects of physical existence into electronic data and digitally processable "information"; in short, each one of them is involved in what we call "the informatization of the body". In order to explain what we mean by this, and why we think it is significant, a brief philosophical detour is required.

A CLASSICAL DICHOTOMY

Below is a list of (in-)famous modernist dichotomies, or dualisms: they come from a philosophical worldview in which everything comes in two, and these two are also each others opposites; more precisely, each pair signifies two fundamentally separate realms:

- reality ↔ language
- referent ↔ representation
- material ↔ immaterial
- biological ↔ social
- "the body itself" ↔ "personal data"
- anatomy ↔ registration/data search
- inside/outside ↔ public/private
- integrity ↔ privacy.

The first four pairs are quite general and abstract; the next four derive from the first four, and are more specific to our case. The primary duality under consideration here, is that of the human body on the one hand, with "personal data", or information *about* that body as its counterpart. This basic dualism resonates with the distinction between reality and language, "the thing itself" and its representation. Whereas the body itself is considered to be a material thing, information about it is not; and whereas the body is presupposed to be a natural entity pre existing the social or the cultural, it is only the way we talk, write, or otherwise represent this body that is considered to be socio-cultural matter.

The last three are not classical dichotomies as such; they relate to the body/data distinction in particular ways. The anatomy/registration pair refers to constitutive or defining technological practices in relation to "the body", and "personal data" respectively; the inside/outside versus personal/private distinctions refer to the crucial boundary in defining the two respective objects; and finally the integrity/privacy pair refers to the key value involved in upholding these boundaries.

It is this habit of dividing everything in two, and declaring them to belong to opposite realms that is the bone of contention here. We suggest it may prevent us from adequately recognizing the profound nature of the changes in the relation between bodies and contemporary technological practices. The current translation of so many aspects of bodily existence into digital data, codes and information, undermines the neat division between the body itself as belonging to material reality exclusively, whereas digital data derived from that body, being mere "representations", are thought to belong to a fundamentally separate domain. We suggest that the developments discussed here actually affect what we presume a body to *be*.

GENETICS: THE PRE-EMINENT EXAMPLE

Thus, through the cumulative effects of a wide range of technologies, sciences, and daily life practices, very gradually a change in our self-understanding as embodied beings is taking place. Ranging from developments in key medical sciences of the twentieth century (endocrinology, immunology, reproductive and genetic science), to the data processing practices of today's medical diagnostics, visualization, therapeutical, and recording techniques, up to the biometric identification and verification processes encountered in daily life, more and more we find our bodies becoming defined in terms of "information". Moreover, this "information" is of a type that renders it processible as digital data. An analysis into the core of our physical being yields an electronically generated genetic profile, just as by interacting with our environment, moving around and touching designated sensoring devices, we leave traces that serve as computer input. We suggest this should be seen as something more profound than constituting yet one more instance of the collection of "personal information", as is more commonly done. Rather, the human body is implicated in a process of co-evolution with technology, information technologies in particular. Within this co-evolution, the ensemble of technologies, sciences and practices of genetics constitutes the most outstanding example, the very epitomization of the new body-as-information. On both the levels of scientific conceptualization and practice there is a strong convergence taking place between genetics and computerscience [6]. With its focus on key concepts like "information", "(de-)coding)" and, eventually, (re-)programming and (re-)combination, one could argue that genetics has become a form of information science. In combination with the popular understanding of genes and DNA as the core, the very essence, of our being and identity ("we are our genes") [7], we see how the genetic body is among the most pronounced instances of the informatization of the body.

The question now becomes how to maintain the distinction between "the body itself" and "information about" that body, if the body itself, in a way, now consists of information? For example, in the chain of biological sample, isolated DNA, DNA records, STR profiles, complete genetic profiles, (what are today believed to be) medically non-coding polymorphisms, and (what are today known as) "health-related loci"....where exactly is the transition from bodily matter to bodily data? Does it really make sense to presuppose a clear distinction?

ETHICAL IMPLICATIONS

Privacy or integrity?

Issues like this are not just academic philosophical puzzles, but have practical and normative relevance. They are partly comparable to the legal and ethical debates concerning the status of prostheses, implants, (donated) organs, gametes, or blood, resulting from earlier forms of technological novelties relating to the treatment of bodies: here too, questions arose on how to define the body's boundaries.

In the case of the body-as-information, the problem is that we have very different concepts, practices, techniques, and institutions for protecting bodies from those protecting information from unjustified access and intrusion, however "personal" that information may be. Whereas in the first case the very integrity of the body is at stake, in the second, the concept of "informational privacy" applies, which carries less moral weight. But this "task division" presumes that it is self-evident what belongs to "the body itself", and where information about the body begins - in other words, this task division runs into trouble here, exactly because this crucial distinction has lost its self-evidence. How can we ensure the integrity of bodies once these bodies assume an extended existence as "information"?

This problem becomes all the more poignant because of the possibilities and particularities of digital data processing. The digital rendering of bodies allows forms of processing, of scrolling through, of datamining peoples' informational body in a way that resembles a bodily search. Beyond mere data privacy issues, integrity of the person, of the body itself is at stake here. Legal and ethical measures and protections should therefore perhaps be modelled analogous to bodily searches, and physical integrity issues.

This issue is of particular relevance with regard to a curious aspect of this new body, namely that it has become *(re-)searchable at a distance*. The digitized body can be transported to places far removed, both in time and space, from the person belonging to the body concerned. Databases can be remotely accessed through network connections; they are built to save information and allowing retrieval over extended periods of time. A bodily search or examination used to require the presence of the person involved – a premise so self-evident that to question it would be quite ridiculous. Moreover, this requirement rendered the idea of consenting to any bodily search at least a practicable possibility. Today, however, these matters are not so obvious any more.

Take again the example of forensic DNA-typing. Lawyers and legal scholars have been very keen to point out the seriousness of the infringement of bodily integrity at stake in taking DNA samples from suspects. Very stringent legal rules have been installed to safeguard the rights of suspects and convicts. But of course, it can hardly be the saliva swab taken from the inner lining of the mouth, or the hair pulled from a sleeve that constitutes such a compromising of bodily integrity. It is not the generation of the body data *per se*, but the information about the body thus gathered, and all the analyses, processing, and knowledge about the person this information makes possible, that is of concern. Moreover, the storage of this information allows researching suspects' bodies over indefinite periods of time. With new analytic techniques becoming available all the time, it will be very tempting to reopen old and unsolved cases, and search the data anew. Under current law, such a search would merely count as a privacy-sensitive data search, whereas we may have to come to acknowledge that it actually amounts to a (new kind of) body search.

In a medical context it is also easy to imagine how, for example, an examination of someone's body's insides can be executed by a "third party" located elsewhere, by remote accessing of digital diagnostic images and data – and without the patient being aware of this. Again, under current regulations, this would merely count as (confidential) data sharing between professionals, whereas it may be better regarded as a virtual physical examination of the patient's body.

Identity and social categorization

Stored, retrievable, and keyword searchable from many different locations, simultaneously or over extended periods of time, these "body data" can become part of information processing practices in ways that were not possible before, or generate new practices altogether. The extensive potential for new forms of knowledge production, policy making and implementation, targeting, and the development of "prevention strategies", is widely welcomed but will also give rise to new forms of surveillance that may not all be just benign.

The biometrically identified bodies at the airport are automatically assessed as either known or unknown, legal or illegal, wanted or unwanted, low or high security risk-assessments with very concrete consequences for the futures of the persons concerned. Similarly, the body defined in terms of its genetic profile, nicotine or medication intake, disease history etc., becomes a body that is assessed as either normal or abnormal, as healthy or pathological, as low or high risk. Particular profiles can be produced from large amounts of data, and social identities affixed to persons behind their backs, whether they actually fit the category in question or not. With the growing interconnectedness of networks, cross-matching of databases, and sharing of information between agencies and institutions, both in the public and private sectors, such attributed identities can become like a person's shadow: hard to fight, impossible to shake.

Thus the informatization of the body reconstitutes identity, and transforms its performance. Our machine readable bodies disclose who we are, in some ways beyond our control, and possibly contrary to our interests and wishes. In forensics, but also for example in border and migration control, identity is established from bodies in ways that bypass what the person in question themselves might say. You may claim to be the daughter of this woman from Sierra Leone, your genetic profile says otherwise; you may say that you're only 14 years old, but the machines X-raying you tell us you are a liar; you may want to convince us that you are this healthy, low risk, person, but our data show you to be quite someone else. In all these examples the outcomes may be reversed: you may after all be able to prove your innocence, your entitlement to enter the country, or your employability.

The machine readable bodies are believed to be more truthful than the speaking persons themselves, who, in the process of being bypassed, are defined as "suspect". These kinds of uses of body data may reinstate forms of determinism by the possibility that life chances and entitlements come to be made contingent upon them.

SOME META PROBLEMS OF ETHICAL DISCOURSE

The approach to the described ethical problems in terms of "privacy" – and to be honest, one in terms of "integrity" as well – even though indispensable and difficult enough to achieve adequate recognition for, entails some problems that need to be addressed as well. Approaches like this suffer from a methodological individualist bias: they remain too much focused on the level of the individual. They define ethical problems in terms of threats, risks and harm to individual persons. This has certain consequences with regard to the possibilities of effectively identifying and addressing some of the ethical issues at stake.

First, it tends to pitch individual interests and rights against collective interests and "the common good". Mostly, this ends in a stalemate between the two; otherwise, and depending on the political climate, the one or the other will lose out. In Western liberal democracies, individualistic values tend to be dominant to an extent that, at least in theory and law, the rights of the individual are not to be subordinated to general or collective interests without very strong reasons.

The second consequence of the individualist bias is that it tends to invoke solutions that are limited to the individual level as well. Generally, this means that any perceived ethical problem is addressed by giving individuals a corresponding right: the right to give, withhold, or revoke consent; the right to be informed; the right to know or not to know; the right to check the accuracy of data, the right to appeal, and so on.

The problem with this is that the possibilities to exercise these rights are largely imaginary. To most people, the precise topography and mechanisms of information systems and networks are totally opaque. It is hardly realistic to expect of individuals to keep track of when and where their rights are potentially being compromised, let alone that they will be able to know how, when, and to whom they should address complaints. In the case of genetics, these problems become particularly pronounced. The very possibility of an *informed* consent, for example, is illusory, when talking about future research or processing of genetic data. It is impossible for people to know, or be told, to what use future research on genetic data will lead. The future is open, and nobody can foresee what kind of knowledge will result, or even what kind of research will be done with the data.

So a common practice is to have people sign a general waiver, foregoing any right of say about all future use of their data. As it turns out, a vast majority of people will agree to sign such a waiver, probably simply assuming that it will contribute to some common good. This way the whole idea of individuals' rights to control their own data, as the privacy protection discourse would have it, becomes rather empty. On the other hand, doing without such general waivers, and really asking people whether they consent to each new use of their data, is hardly realistic either. If you have a database with data on thousands of people, and you, as a researcher, want to do some mining or analysis, you simply cannot realistically go back to each individual and ask them whether they agree with your research project. This would seriously undermine any positive use of such databases for purposes most people agree would be very beneficial for the community. The result is either a wide disparity between normative and ethical ideals and the actual practices and uses of these databanks, or a limitation on such use so strong that the possibilities to derive societal benefits form them is severely impaired.

This unsatisfactory situation can be approached from another angle however. The culprit causing this problem, according to Dutch philosopher Tsjalling Swierstra in a recent article [4], is a dysfunctional adherence to an ethical paradigm or discourse that, in the context of the challenges posed by today's DNA-banking, is somewhat obsolete. He calls this the "discourse of defence". It generates from ethicists' individualistic bias, and results in the tendency to solve any ethical problem with giving individuals more rights, however impractical, or unrealistic, and even unappreciated by these individuals this might be – for in general people are not at all that much interested in the kind of informed consent and privacy issues. This discourse of defence assumes that the main ethical problem lies in protecting individuals against harm from knowledge of other, more powerful actors, about their genetic make-up. This, he claims, stems from the era, when monogenetic diseases were still the main focus, and everybody still expected that the main outcome of further genetic research would result in an ever longer list of such monogenetic abnormalities in individuals. Knowledge like that would imply a certain verdict about one's future, that, when known to third parties, could seriously harm and stigmatize, invoking all kinds of discrimination.

As we described above, this expectation has changed. Most afflictions and personal characteristics have turned out to be the outcome of complex interactions between many genes, and other, environmental factors, so the dangers of disclosure turned out to be exaggerated. There is no simple causal line from one specific genetic profile to one specific disease or characteristic, or at least these are the exception. More common is a profile, shared with many others, that merely indicates a predisposition, a hard to define chance of developing certain traits and not others. Therefore, we could perhaps afford to look for an alternative to this discourse of defence, that besides the disadvantages already mentioned, places the burden of constant vigilance, and of remaining informed about complicated issues on the shoulders of the individual. Instead of individuals as permanently threatened victims, Swierstra suggests, a new focus could be on the "organization of solidarity" in society, so that citizens need not fear abuse of their genetic material, or other body data, but can trust that this will serve the purposes they assumed it would when they altruistically donated them. This would lift part of the need for protection from the overburdened individual, in exchange for which a restriction of the right to revoke or withhold their consent at every corner and step of what, from society's viewpoint, constitute beneficial practices and research projects. For example, when donating DNA samples for a dragnet search in a criminal investigation, or for highly promising medical research, the right to revoke consent would give way to society's justified need to catch dangerous offenders, or search for knowledge about lethal diseases. In exchange for this, the burden of ethical justifiability would then shift to architectural, organizational, and legal structures of the databases. Swierstra offers the example of databanks legally and organizationally structured as charitable trusts (rather than private property, to be exploited for profit), with the possibility of donors becoming board members with voting rights on what research, and whose access to the data to endorse. This makes it easier for citizens to contribute to the common good when needed, instead of remaining focused on self protection in a threatening world. Actually, it would take into account the fact that most people do not worry too much about their privacy, and, rightly or wrongly, assume that somehow giving information about themselves serves some common good. An ethical focus on citizenship rather than individual privacy rights would then try to make sure that this trust is warranted.

To what extent such alternative forms of organization are practically realizable in cases like police DNA-banks and other security sensitive databases is an open question. There is, however, a good point to derive from this proposal that does pertain to the collection and storage of body data more generally. In order to get beyond an ethical analysis emphasizing once more the need to protect individual privacy, a more fruitful direction for a constructive ethical contribution to shaping future arrangements in an ethically just way may lie in a shift of focus towards analysis of technical infrastructures and intermediary institutions. Some database architectures, technical standards, authorization structures, or forms of interoperability may be more conducive to transparency and democratic control than others. If the informatization of bodies is to serve both community and individual interests, while simultaneously offering protection of the common good and the integrity of the body, ethical vigilance must move to another level.

Submitted on invitation.
Accepted on 4 October 2006.

References

1. Van der Ploeg I. Biometrics and the body as information: normative issues in the socio-technical coding of the body. In: Lyon D (Ed.). *Surveillance as social sorting: privacy, risk, and automated discrimination*. New York: Routledge; 2002. p. 57-73.
2. Rodota S. Body transformations. *Law Hum Genome Rev* 2004(21):29-47.
3. Wellcome Trust. Forensic DNA databasing. A European perspective. In: *Welcome Trust, 2005*. Available: from http://www.dur.ac.uk/p.j.johnson/eu.html; last visited june 2005.
4. Swierstra T. Een tumor is ook collectief bezit. Het afstaan van lichaamsmateriaal ten behoeve van DNA-banken. *Krisis* 2004;5(4):36-54.
5. Weiss MJ. Beware! Uncle Sam has your DNA. Legal fallout from its use and misuse in the US. *Eth Inform Technol* 2004;6:55-63.
6. Marturano A, Chadwick R. How the role of computing is driving new genetics' public policy. *Eth Inform Technol* 2004;6:43-53.
7. Dÿck Jv. *Imagenation. Popular images of genetics*. New York: New York University Press; 1998.