scanners. The question is not just about using or not using a certain kind of security technology. There are also issues of how to minimize undesirable side effects and establish adequate regulations.

Unfortunately, the example of body scanners also points to the limitation of privacy-by-design, because advanced imaging technologies still identify people with nonvisible disabilities or with medical conditions as "suspicious." This example points up the often overlooked tension between security and justice (Ammicht Quinn and Rampp 2009).

Authors such as Rosen are a little bit too optimistic about the ability to minimize tensions between security and other human values. As Mark Neocleous (2007) has pointed out, the idea of a balance between security and liberty is a myth; security is always the "real political trump card" (Neocleous 2007, 144) in Western liberalism. This dominating character of security is one reason why Wæver and others have argued in favor of "desecuritization"—that is, removing an issue from the arena of security concerns. A successful desecuritization move might also open up new ways of addressing an issue from a long-term perspective.

Helen Nissenbaum's 2005 paper "Where Computer Security Meets National Security" is one of the few examples in applied ethics in which an explicit connection is made between ethical issues of security and security in the field of international relations.

Ethicists focusing on security technologies do not need to become experts in security studies. It might be advisable to take a two-level approach that not only focuses on how to pursue security ethically but also critically examines the underlying concept of security.

SEE ALSO *National Security; Security Technologies.*

BIBLIOGRAPHY

Ammicht Quinn, Regina, and Benjamin Rampp. 2009. "The Ethical Dimension of Terahertz and Millimeter-Wave Imaging Technologies: Security, Privacy, and Acceptability." *Proceedings of SPIE* 7306, Optics and Photonics in Global Homeland Security V and Biometric Technology for Human Identification VI, 730613 (May 5).

Bynum, Terrell. 2011. "Computer and Information Ethics." In *The Stanford Encyclopedia of Philosophy*, Spring ed., edited by Edward N. Zalta. http://plato.stanford.edu/archives/spr2011/entries/ethics-computer/

Hobbes, Thomas. 1929. *Leviathan*. Reprint from the edition of 1651. Oxford, UK: Clarendon Press.

Hobbes, Thomas. 1983. *De cive. The English Version*. Edited by Howard Warrender. Oxford, UK: Clarendon Press.

Moor, James H. 1997. "Towards a Theory of Privacy in the Information Age." *Computers and Society* 27 (3): 27–32.

Neocleous, Mark. 2007. "Security, Liberty, and the Myth of Balance: Towards a Critique of Security Politics." *Contemporary Political Theory* 6 (2): 131–149.

Nissenbaum, Helen. 2005. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7 (2): 61–73.

Rosen, Jeffrey. 2004. *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*. New York: Random House.

United Nations Development Programme (UNDP). 1994. "New Dimensions of Human Security." In *Human Development Report 1994*, 22–46. Oxford: Oxford University Press. http://hdr.undp.org/en/media/hdr_1994_en_chap2.pdf

Wæver, Ole. 1995. "Securitization and Desecuritization." In *On Security*, edited by Ronnie D. Lipschutz, 46–86. New York: Columbia University Press.

Michael Nagenborg

SECURITY TECHNOLOGIES

Following Bruce Schneier (2003, 11), security "is about preventing adverse consequences from the intentional and unwarranted actions of others." This definition nicely captures some of the characteristics of the understanding of security in current Western discourses: (1) Security is thought of something to be provided and maintained. Security is about "doing something" (Molotch 2012). (2) Security is about preventing future events. (3) Security measures might infringe on the freedom of others.

It is common to differentiate between *security* and *safety*. Whereas safety addresses accidents, natural disasters, and human-made catastrophes, security deals with attacks and (serious) criminal acts. As Langdon Winner has argued in "Technology Studies for Terrorists: A Short Course" (2006), however, there is considerable overlap with regard to technology design, because any unintentional damage may as well be brought on intentionally. This also holds true for disaster preparedness. Being able, for example, to provide medical support to a large number of casualties is as helpful in case of a natural or human-made disaster as it is in case of a terrorist attack.

A TYPOLOGY OF SECURITY TECHNOLOGIES

Because of the overlap between safety and security in the area of disaster preparedness, the focus of the following typology is on technologies that are being used to *prevent* attacks. Weapons are outside the scope of this entry, because they raise additional and different ethical issues. But the use of military technology in the context of security is briefly addressed in the final section.

Limiting the options of others is a fundamental principle in providing security. Therefore, controlling the access to places and resources (including information) has become a central security issue. For example, keys and locks allow restricting the access to a certain place or

specific goods to the possessor of the key. Yet because everybody who gets the key will be able to open the lock, the key becomes yet another asset to be protected. This example shows that (new) security technologies might very well create (new) security issues and insecurities. Furthermore, it is often assumed that the person who secures something is entitled to do so. But thieves may use locks and keys to protect their stolen goods, too. Security technologies may also go along with vigilantism. The latter point has been raised, for example, with regard to digital rights management systems (Lipinski and Britz 1999).

With regard to information security the use of cryptographic technologies has a similar function as keys and locks. One may not be able to stop a third party from intercepting a message, but one might prevent access to its content. In fact, "the advances in cryptology during the first three centuries of the Islamic civilisation" have been attributed in part to "a high level of public literacy" (Strasser 2007, 279). There is little need to protect written messages if there only are a few people who are able to read them. Encrypting documents is also a way to protect their integrity and authenticity.

An encrypted message may also be used to authorize the messenger by establishing a link between the content of the message, the cipher being used, and the messenger. From an ethical perspective it is worth noting that in such a case trust in a person is established by trusting in a sociotechnological system. Hence, it is crucial to ask how security technologies do shape and mediate interactions between human beings (Monahan 2006). This holds especially true for biometric technologies that are being employed to establish a link between certain features of a person's body and a document or an information system (van der Ploeg 1999; Aas 2006).

Surveillance technologies might be used in some contexts to promote security. For example, the employment of closed-circuit television (CCTV) systems increases the likelihood of attackers being identified after they have committed a crime, and thus they may serve to deter some crimes from being carried out. Of course, such technologies provide little protection against suicide bombers. Therefore, one of the key challenges in the area of surveillance technologies is to identify attackers before they carry out an attack. Systems (e.g., facial recognition systems) may be designed and employed to recognize known dangerous or suspicious persons. These systems, however, raise serious concerns with regard to privacy and justice (Brey 2004; Introna and Wood 2004). Advanced systems are even designed to detect dangerous situations based on more abstract pattern-recognition algorithms. While these technologies (e.g., smart CCTV or data mining technologies) are currently mostly used to assist human security personnel, they still are being questioned with regard to the protection of civil rights as well as to the degree of the autonomy and hence responsibility of the system.

Finally, new detection systems have arisen that aim to extend and complement the range of human senses. For example, advanced imaging technologies (such as body scanners) enable users to detect concealed objects under clothing. Some ethical issues have been addressed by following the privacy-by-design principle (Rosen 2004). These technologies, however, still place a great burden on people with hidden disabilities and in certain medical conditions, because they get marked as suspicious (Ammicht Quinn and Rampp 2009).

As has become apparent in the example of the body scanner, security technologies need to be evaluated not only with regard to their impact on privacy and liberty but also from the perspective of justice. Given the (pro)active understanding of security today, it is therefore necessary to ask what kind of security is provided to whom—and who pays the price for these security measures.

DUAL-USE TECHNOLOGIES

At least in Europe, the transfer of knowledge and technologies from the military to the civil sector (and vice versa) has given rise to concerns about the militarization of everyday life (Graham 2010). While one must take into account the different perceptions of the military in different cultures and countries, the international debate on unmanned aerial vehicles (also known as drones) demonstrates the general unease about the use of military technology for security purposes (Finn and Wright 2012).

Besides concerns about the growing influence of the defense sector on shaping research agendas (see, e.g., Hayes 2006), there are at least two issues to be taken into consideration from the perspective of the philosophy of science and technology. Because the research and development of military technology is often perceived as a matter of national security, there is a lack of transparency. While the issue of secrecy as a means to promote national security also arises in other areas of research, the use of military technologies in a civil context might increase the barriers for critical inquiries. And this becomes even more important if one does not consider technologies to be mere "neutral" tools.

SEE ALSO *Biometrics; National Security; Security, Concept and History.*

BIBLIOGRAPHY

Aas, Katja Franko. 2006. "'The Body Does Not Lie': Identity, Risk, and Trust in Technoculture." *Crime, Media, Culture: An International Journal* 2 (2): 143–158.

Ammicht Quinn, Regina, and Benjamin Rampp. 2009. "The Ethical Dimension of Terahertz and Millimeter-Wave Imaging Technologies: Security, Privacy, and Acceptability." In *Optics and Photonics in Global Homeland Security V and Biometric Technology for Human Identification VI*, 13–16 April 2009, Orlando, Florida, edited by Craig S. Halvorson, Šárka O. Southern, B. V. K. Vijaya Kumar, Salil Prabhakar, and Arun A. Ross, 1–11. Proceedings of SPIE—the International Society for Optical Engineering 7306, Bellingham, WA: SPIE.

Brey, Philip. 2004. "Ethical Aspects of Facial Recognition Systems in Public Places." *Journal of Information, Communication, and Ethics in Society* 2 (2): 97–109.

Finn, Rachel L., and David Wright. 2012. "Unmanned Aircraft Systems: Surveillance, Ethics, and Privacy in Civil Applications." *Computer Law and Security Review* 28 (2): 184–194.

Graham, Stephen. 2010. *Cities under Siege: The New Military Urbanism*. London: Verso.

Hayes, Ben. 2006. *Arming Big Brother: The EU's Security Research Programme*. Amsterdam: Transnational Institute; London: Statewatch.

Introna, Lucas D., and David Wood. 2004. "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems." *Surveillance and Society* 2 (2–3): 177–198.

Lipinski, Tomas A., and Johannes J. Britz. 1999. "Intellectual Property in the 21st Century: A Return to the Underlying Ethics and Information Ownership and Dissemination." *Ethics and Justice* 2 (1): 3–8.

Molotch, Harvey. 2012. *Against Security: How We Go Wrong at Airports, Subways, and Other Sites of Ambiguous Danger*. Princeton, NJ: Princeton University Press.

Monahan, Torin. 2006. "Questioning Surveillance and Security." In *Surveillance and Security: Technological Politics and Power in Everyday Life*, edited by Torin Monahan, 1–23. New York: Routledge.

Rosen, Jeffrey. 2004. *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*. New York: Random House.

Schneier, Bruce. 2003. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York: Copernicus Books.

Strasser, Gerhard F. 2007. "The Rise of Cryptology in the European Renaissance." In *The History of Information Security: A Comprehensive Handbook*, edited by Karl de Leeuw and Jan Bergstra, 277–325. Amsterdam: Elsevier.

van der Ploeg, Irma. 1999. "Written on the Body: Biometrics and Identity." *Computers and Society* 29 (1): 37–44.

Winner, Langdon. 2006. "Technology Studies for Terrorists: A Short Course." In *Surveillance and Security: Technological Politics and Power in Everyday Life*, edited by Torin Monahan, 275–291. New York: Routledge.

Michael Nagenborg

SELFISH GENES

Evolutionary biologists increasingly accept that genes are *selfish*. But what does this mean? Clearly genes do not have personal motivations, and even if they did, they could not achieve their designs without cooperation of the bodies in which they reside. In the most general sense, genes are merely blueprints, or, better, recipes, for the production of proteins. As such they influence the anatomy and physiology of living things including not only structural proteins but also enzymes and other factors that underlie the functioning of organisms. Genes ultimately affect, for example, the structure of kidneys, as well as the structure of nervous systems. Genes thus influence kidney function, just as they influence central nervous system function. When the central nervous system functions, behavior results. In this sense, genes are intimately connected to behavior, no less than they are to the physiology and anatomy of our internal organs.

Organisms are typically rather short-lived. Although they occupy the most obvious stage of the ecological and evolutionary theater, and natural selection appears to act on organisms whenever some reproduce differentially relative to others, the fact remains that natural selection among organisms is only important in the evolutionary sense insofar as it results in the disproportionate replication of some genes relative to others. Individual bodies themselves do not persist in evolutionary time; genes do. In fact, genes are potentially immortal whereas bodies are not.

SELFISH GENES AND MODERN GENETICS

At the time of Charles Darwin (1809–1882), genetics was unknown, and so the focus of early evolutionary biology was on bodies. With the rise of Mendelian genetics and, subsequently, the field of population genetics, it became possible to trace the consequences of differential reproduction on their ultimate units, the genes themselves. Recognition of DNA as the genetic material, along with identification of its structure and the rise of modern genomic technology, has enhanced our understanding and also clarified the importance of focusing on these crucial units. When a hippo or a human being has a certain fitness, this means that his or her DNA is projected into the future with a given degree of success.

The term *selfish*, in relation to genes, is no more than a useful verbal shorthand. Selfishness simply refers to success in contributing to a particular gene's own replication. Natural selection rewards those genes that produce a *successful body* by causing more of the genes that influence the production of that body to be projected into the future. In this regard a successful body is one that metabolizes efficiently, that pumps blood successfully, that regulates its internal environment in a way conducive to life, and that also behaves in a manner that maximizes its success in reproducing, and/or in contributing to the reproduction of its component genes in the other major way available to it: by contributing to the success of genetic relatives, with the importance of each relative devalued in proportion as it is