




The problems of privacy and its protection are, of course, not confined to (applications of) nanotechnologies. But privacy issues are intensified by nanotechnological developments; therefore privacy is one area of investigation and concern in the field of  nano-ethics.



The distinction between politics as a public sphere and the domestic private sphere of the family can already be found in ancient Greek philosophy, namely in Aristotle's writings. Here two domains are defined: one is personal, 'privatus' (Latin), which means deprived from the public, not open. The other is public (Latin 'publicus') which means open, common, accessible (rather unrestricted).

Other theories rather emphasize the opposed domains as one that is subject to state control and on that is left to 'self regulation' (in a very broad sense) or the right to be left alone. Another focus is 'informational privacy' that emphasizes the element of control over information about oneself as an extension of the classical "my home is my castle"-conception of privacy in the face of modern technologies. Prosser (1969: 389) defined four privacy rights:

1. Intrusion upon a person's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about an individual.
3. Publicity placing one in a false light in the public eye.
4. Appropriation of one's likeness for the advantage of another.



The history of theories about privacy is long, and different times have laid different emphasis on the concept. However, basic ideas about privacy nowadays are formulated e.g. in the "Convention for the Protection of Human Rights and Fundamental Freedoms" (Council of Europe, September 2003, esp. Art. 8;10) – of course immediately followed by exceptions: "except such as

is in accordance with the law and is necessary in a democratic society in the interests of national security, ..." (Art. 10,2).



In the philosophical discourse there is no agreement whether privacy issues really are morally distinctive and form a separate, coherent concept (coherentism), or whether they are reducible to claims of other sorts like property interests or infliction of emotional distress and thus are no category of their own (reductionism). For the analysis in the context of nanotechnologies it denotes an established set of concerns that are treated as a coherent field of investigation.

Other criticisms concerning privacy, for example from a feminist point of view, point out the 'darker side' of privacy, because it can also be used to cover up domination or abuse behind a privacy shield.



### Meaning of privacy


Concerning the value privacy has for individuals or groups, different approaches can be distinguished:

- (1) Privacy is the control over information about us that is communicated to others. It is also control over *access* to private places, information etc.

- (2) The social value of privacy is an 'inviolate personality'. "It defines one's essence as a human being and it includes individual dignity and integrity, personal autonomy and independence. Respect for these values is what grounds and unifies the concept of privacy" (DeCew 2006). Therefore invasion of privacy is an affront to human dignity.

- (3) Another view argues that privacy and intimacy are closely related. Without privacy no individual could experience close relationships, privacy invasions destroy intimacy and – social relations.



Another hard-fought question is whether privacy is relative. Different cultures may have different standards or definitions 

☞ of privacy. Which elements are 'universal', which are 'relative'?



In the case of nanotechnologies, as potentially with all technologies, the focus of the debate is the question of control over information respectively the control over access to information, places and other personal realms. The major area of interest then is surveillance technology, but also diagnostic instruments and data in health care.

Surveillance has become a major issue, not only since the terror attacks of 2001. Cameras proliferate in public buildings, on streets and places. Internet data transmissions are recorded, phone calls tapped. Since nanotechnologies serve to miniaturize the technical equipment, surveillance could become more pervasive and more miniaturized even than RFID chips. This affects surveillance in public places and buildings, but also the surveillance in private places.

Moreover, since scientists and economists promise that the new technologies, once they are on the market, will be much cheaper than before, the access to more sophisticated means of surveillance will not be restricted to authorities (which might be worrying enough). Professional surveillance might also be employed by individuals, companies, criminals etc. How can privacy be protected in this scenario?

In health care, research promises smaller and better sensors and labs-on-a-chip, which would yield much more data at lower costs concerning the health status or

genes of patients. While it certainly is good to be able to detect illness at an early stage and monitor the health status of a patient more thoroughly, identifying problems that hitherto were only recognized when it was too late, there will also be a huge amount of data concerning a patient that has to be protected – from the eye of the public, the insurances, criminals and so on.

Two more general questions: If the development of technology leads to more and more sensors, chips etc. that control functions of the environment in our everyday life (Ambient Intelligence), and if this technology will be invisible to the eye to the extent that we are not aware of it anymore – will this change our notion of privacy?

Will the greater possibilities of surveillance lead to a shift in the balance of privacy and security? Would we be willing to trade privacy for more security? Would individuals use surveillance to know where their dog, husband, wife ... is?



**Q:** Today we are already surrounded by a lot of technology. What would be different with Ambient Intelligence? **A:** Today, on most gadgets there is still an on/off button, AI doesn't need something like that anymore. While current technology has to be handled by us and is clearly 'visible' when you look for it, with AI the environment becomes 'opaque' and takes away control from us.



STEFAN GAMMEL

---

## 📖 Links to other Portfolio sheets:

📖 Nano-Ethics    📖 Ethics and Morality

## 🕒 Literature: Print & WWW

DeCew, Judith, "Privacy", The Stanford Encyclopedia of Philosophy (Fall 2008 Edition), Edward N. Zalta (ed.), URL = <<http://plato.stanford.edu/archives/fall2008/entries/privacy/>>.

Van den Hoven, Jeroen, "Nanotechnology and Privacy, Instructive Case of RFID", In: Fritz Allhoff, Patrick Lin et al.: Nanoethics: The Ethical and Social Implications of Nanotechnology. Wiley 2007.

Toumey, Chris, "Privacy in the Shadow of Nanotechnology", Nanoethics 1(3) 2007, pp. 211--222.