The Next Step: Privacy Invasions by Biometrics and ICT Implants

Karsten Weber

University of Opole, Poland / European University Viadrina Frankfurt (Oder), Germany
kweber@euv-frankfurt-o.de

1. Introduction[1]

Early summer 2005 the Conference of Computer Ethics: Philosophical Enquiry (CEPE) took place in Enschede, The Netherlands. There, a couple of participants of the conference presented papers about so-called "convergence technology" which means that ICT and life sciences are converging – it is supposed that some day there will be no real difference of ICT and biologically or genetically engineered artifacts. One of those speakers argued that it is inevitable that people will use that technology – for example ICT implants. But strangely and to the discomfort of most of the other participants he refused to give another moral justification than merely the statement that it is up to the people whether or not to use such technology. It seems that he was not aware of the fact – or maybe refused to see it – that such technology can produce a couple of severe problems on the medical as well as on the social side.

From the point of view of an ethicist it is quite unsatisfying to merely say that it is up to the people to decide whether they want to use a certain technology like ICT implants or not. Of course, in political philosophy, libertarians argue that the state and its institutions are not entitled to infringe the rights of citizens in general and particularly with regard to the use of technology. Nevertheless, even libertarians would concede that such use can inherit moral problems in those cases that rights of others are concerned. Then, even from a libertarian point of view, the state and its institutions are entitled and obliged to protect the rights of its citizens.

That indicates that it must be possible to get some more detailed and – much more important – better established moral justifications by looking on arguments of political philosophy and ethics. Since political philosophy is a really large field it is necessary to focus on some particular positions. Therefore, in this paper only libertarian, liberal, and communitarian arguments will be addressed to give answers how society should deal with ICT implants. But I won't focus merely on ICT implants but shall take a look on biometrics, too. Biometrics promises that it allows identification without any further artificial feature that the person to be identified has to carry with her. With regard to privacy infringements that inherits that everybody can be recognized and identified everywhere just by characteristics of the person herself – supposed that the necessary identification technology is ubiquitously disseminated. At the end of my paper I will conclude that either libertarian/liberal or communitarian arguments necessarily will support a kind of "democratic" Big Brother scenario.

2. Recent and current ICT and the development of ICT implants

If one takes a closer look to recent and current ICT one will learn that all devices have one characteristic in common: All those devices remained external to the human body. Although they are shrinking in size they do not invade our bodies. Of course, they were built to enhance our information-processing and communication capabilities but they did not enhance or alter our bodies. As one consequence of this strict distinction of ICT and our bodies, most times, human-computer-interaction was a more or less good compromise – as probably everybody knows: CRTs, LCDs, keyboards, and the like are of course useful but have some disadvantages, too.

Now, current developments of ICT show a common direction. ICT devices like computers, mobile phones, GPS receivers, and the like are getting smaller and smaller. We will wear those devices somehow like clothes or even jewelry instead of handling them like external tools. One important advantage of this development is that human-computer-interaction will be improved. But still, these artifacts remain external to the human body. Now, state-of-the-art research is going to make the final shift. The next logical step is that ICT will be integrated in our bodies. Scholars like Kevin Warwick, who works in the UK, already now are conducting research on ICT implants (e.g. Warwick 2003; Warwick, Gasson 2004). He developed several devices which are able to transmit neural signals to control other external ICT devices. The big advantage of such implants is that human-computer-interaction is going to happen "natural" – now, it will be more or less like using the own limbs than using an external tool. However, there are probably some disadvantages, for instance the risk of infections, scars, and the like.

It is very likely that the near future of ICT implants will be characterized by devices used for personal identification. Even now, there are some applications of RFID like implants injected right under the skin. For instance, they are used to localize elderly and/or mentally handicapped persons in old people's homes to prevent these persons from being lost or helpless at some place where nobody can find them. Another application is to use such implants to identify persons in bars or clubs. The RFID chip under the skin identifies them at the point of sale of – for instance – drinks.[1] All other applications that currently are discussed are more or less Science Fiction. Artificial senses, enhancement of central nervous system capabilities, and the like still are far from realization. However, it is possible to project at least one feature that such implants probably will have: the capability to communicate with other devices outside the body of the implant carrying person. Therefore, it will be necessary that these implants can be identified reversibly unambiguous; this is required by communication protocols. Consequently, all these implants will identify themselves and, at the same time, the implant carrying person.

3. Biometrics

Compared to available ICT implants current state-of-the-art technology using biometrics to identify persons is far more sophisticated. There are much more already existing technologies, pilot programs, and real life applications of biometrics compared to ICT implants. In principle, using biometrics implies that some physiological or behavioral characteristics are used to identify a person. To do that, first it is necessary to conduct an initial registration of a person to create "an individual biometric template" (Furnell, Clarke 2005: 9). From then on, it is possible to identify this person "by comparing an acquired sample against the template that is already held." (ibid.) Although in the literature it is stressed that identification on the one hand and verification of identity on the other hand must be distinguished sharply due to substantially different technological challenges, here this difference won't be taken into account.

One will find many different technologies related to biometrics (e.g. Furnell et al. 2000: 531; Clarke, Furnell 2005: 524-526). It is very likely that most people know at least one or two of them but at the same time it is very likely, too, that they do not know much more. Particularly retinal scanning, as well as voice verification, has a high degree of publicity due to their appearance in a couple of blockbuster motion pictures. Retinal scanning, for instance, plays a major role in the James-Bond-sequel "Never say never again", already made in 1983.

Method		Description
Physiological	Face recognition	Uses a camera to take a snapshot of the users face. Key measurements are extracted from the image and are compared to the stored ‘faceprint’.
	Facial thermogram	Uses the varying temperatures emanating from different regions of the face to provide the basis for characterizing individuals.
	Fingerprint recognition	Uses optical, capacitive or thermal techniques to assess the characteristic patterns of forks and ridges in the print that can distinguish one person from another.
	Hand geometry	Measures the physical dimensions of the hand (e.g. span, length of fingers) when spread on a flat surface.
	Iris scanning	A snapshot of the user’s iris, taken by a camera, is compared with a previously stored image.
	Retinal scanning	Uses a laser to scan the distinctive patterns on the retina at the back of the eye.
	Vain checking	Uses infra-red light to enhance the visibility of characteristic vein patterns in the back of the hand.
Behavioural	Gait recognition	Characterises individuals be the way in which they walk.
	Keystroke analysis	Monitors typing activity in order to determine characteristic rhythms. Can be performed on the basis of know text (e.g. in conjunction with a username and password) or upon keyboard inputs in general
	Mouse dynamics	Monitors mouse-related activity, and attempts to characterise users on the basis of measures such as speed and accuracy.
	Signature analysis	Assesses a handwritten signature captured using a special pen and/or pad. Static analysis simply assesses the resulting pattern, whereas dynamic systems also measure the pressure and speed of the signature.
	Voice verification	A user’s voice compared with a previously stored ‘voiceprint’. Can be performed on a text-dependent basis, when speaking a known word or phrase, or text-independently.

Physiological and behavioral characteristics used by biometrics (taken from Furnell, Clarke 2005: 9)

However, often what seems to be a retina scanner actually is an iris scanner which is a quite different technology that easily can be outwitted with simple means like a photo taken with a Polaroid camera (Forte 2003: 13). Voice verification and, probably, face recognition, too, often are shown in motion pictures. But it is very likely that all other technologies presented in the table above are not widely known. Nevertheless, the entries already indicate that many human physiological and behavioral characteristics can be used to identify persons.

3.2 Biometrics and ubiquitous computing

Although ubiquitous computing is not a central issue of this paper it briefly shall be mentioned in the context of biometrics. Current ICT already reduces one's informational privacy massively as Barrera and Okai (1999: 1) stress:

> "To be in cyberspace is to be recorded. Digital activities and objects are nothing but an ensemble of traces and records. […] Those digital footprints can be, by nature, reconstituted, recreated and saved indefinitely. Where a vast number of activities in traditional space are inherently non-traceable, cyberspace actions are the traces themselves."

If we leave a physical space, e.g. a bench in a park, it is almost impossible to track us. Leaving a place in real space in principle means to leave it forever; being in cyberspace however implicates, generally speaking, to be there forever because everything one ever have done there can be tracked. Now, furnishing real space with ICT is going to change how we can act in real space because it then will have characteristics of cyberspace – in principle every real-life action will be tractable indefinitely. Thus, the advantages ICT provides to us could be overridden by the disadvantages of infringements into our privacy, as Leonhardt and Magee (1998: 52) emphasize with regard to location-based services:

> "[…] location services will often become repositories of potentially sensitive personal and corporate information. *Where you are* and *who you are with* are closely correlated with *what you are doing*. To leave this information unprotected for everybody to see is clearly undesirable."

Mobile ICT and ubiquitous computing environments cannot work without identification and localization of users due to the aim of such systems to provide location- and context-aware services. In order to adequately react to our requests service and content providers continuously have to know about our actions, behavior, and lifestyle. Now, biometrics can provide the means for identification and authorization of users without any extra activity of them and even without their consent. Therefore, the idea of ubiquitous computing environments does not make sense without biometrics. Implicitly, if one talks about ubiquitous computing one always talks about biometrics, too.

4. Public and private application of ICT implants and biometrics

One important distinction has to be drawn when ICT implants and biometrics are at stake. Such technologies can be applied for private and for public aims and they can be used in private and public contexts. But, although one can make that distinction on an analytical level, in real life it is difficult to draw a line between private and public contexts and between private and public aims.

To make that point more clear, suppose a scenario: In the near future a company will offer a combination of biometrics and ICT implants for personal protection purposes – just for fun, let us call it “π^3″ (Blythe et al. 2004 mention wearable computing technologies as means to protect elderly people against crimes). Implanted sensors and transmitters continuously will send information about body functions like blood pressure, temperature, heart beat frequency, and the like to a medical supervisor device. Furthermore, the exact geographic position of that person and information about the environmental conditions at the location like humidity, air temperature, noise level, and so on will be transmitted (Prekop, Burnett 2003: 1169). In case of critical conditions security personnel will be alarmed. Probably, many of us will appreciate such technology, particularly those of us who have permanent health problems or suffer from chronic diseases. And of course, it is a legitimate aim to protect oneself from damage. Therefore, it seems to be difficult to argue against the application of such technology. But even in this version of the scenario not only the person carrying that system is affected but other people, too. For instance, if the system will monitor environmental parameters, in combination with its carrier this system is a perfect mobile control device. Additionally, let us suppose that it is combined with biometrics capable to identify persons who approach the carrier. Obviously, for persons at risk this would be an opportunity of protection. But at the same time it is a perfect means of supervision. Now, a private aim becomes of public importance.[3]

5. Political philosophy in general

Technologies like those addressed in this paper often are discussed with regard to issues like "Big Brother" and "Panopticon" (e.g. Lyon 2001; Patton 2000; Pecora 2002). Roughly speaking, the term "Big Brother" refers to a state which will control the whole life of its citizens. In contrast to that, "Panopticon" refers to a society in which everybody is controlling continuously anybody else. Therefore, "Big Brother" more or less implies a totalitarian state and society whereas a "panoptic" society could be democratically governed. Nevertheless, with regard to a Big Brother as well as to a panoptic society one can raise the question whether and how civil rights can be protected. Of course, the Big Brother scenario seems to imply that no civil rights at all are granted – particularly because we all know George Orwell's famous book "1984". But with respect to a panoptic society, too, one can ask whether and which civil rights can be protected, although the Panopticon is compatible with a democratic society. I will roughly discuss that question in relation to libertarian, liberal, and communitarian arguments. Of course, it would be necessary to discuss utilitarian positions, too, but I won't do that due to one simply reason: Roughly speaking, from a utilitarian point of view civil rights are no absolute constraints to state action. If the application of biometrics or ICT implants would increase the net utility of a large number of persons it would be quite difficult to argue against their application from a utilitarian point of view. Utilitarianism inherits infringements into civil rights of the few if it is possible to maximize the net utility of the many – we all can learn that lesson from the debates on terrorism and torture.

5.1 Libertarian and liberal positions[4]

For libertarians, rights are exhaustive which means that they are absolute constraints to the actions of other people. As Isaiah Berlin (2002) puts it they draw a line around a person which marks a border that nobody is entitled to cross. The state and its agents, too, are not entitled to make infringements in those rights, as Robert Nozick (1974: IX) stresses:

> "[…] a minimal state, limited to the narrow functions of protection against force, theft, fraud, enforcement of contracts, and so on, is justified; that any more extensive state will violate persons' rights not to be forced to do certain things, and is unjustified; and that the minimal state is inspiring as well as right. Two noteworthy implications are that the state may not use its coercive apparatus for the purpose of getting some citizens to aid others, or in order to prohibit activities to people for their *own* good or protection."

In strong contrast to communitarians, libertarian scholars emphasize that mere moral concern of other people is no reason to make infringements in the rights of persons:

> "So how do we judge disputes between rights and other values? […] In so far as we are talking about enforceable obligations – those we may legitimately enforce by sanction of punishment – rights are exhaustive. Our only enforceable moral concerns are based on rights. Thus private property rights, for example, will always take moral priority over considerations of archaeological value. […] It would be a great pity if property developers built an office block on top of ancient remains. But if the developers legitimately own the site, then they have a perfect right to build on it even if the result is the destruction of something of great value." (Wolff 1991: 22/23)

The utilitarian and communitarian idea that the state must protect and propagate the common good of a society is alien to libertarians as well as to liberals:

> “Justice is the first virtue of social institutions, as truth is of systems of thought. A theory however elegant and economical must be rejected or revised if it is untrue; likewise laws and institutions no matter how efficient and well-arranged must be reformed or abolished if they are unjust. Each person possesses an inviolability founded on justice that even the welfare of society as a whole cannot override. For this reason justice denies that the loss of freedom for some is made right by a greater good shared by others. It does not allow that the sacrifices imposed on a few are outweighed by the larger sum of advantages enjoyed by many.” (Rawls 1999a: 3/4)

Putting this together, a simple and concise idea crystallizes: On the one hand, the state and its agents must protect the civil rights of citizens. On the other hand, state authorities are not entitled to make infringements into those rights to support a certain conception of a good live and there is no entitlement to support a common good; in fact, libertarians – and somehow liberals – even do not know what the “common good” might be. Libertarians – and a lot of liberals, but certainly not all of them (e.g. Raz 1994: 29) – believe that only persons are right-holders (e.g. Narveson 2001: 14); for them, groups or society merely are metaphysical conceptions and cannot be right-holders. Therefore, a mandatory use of ICT implants or biometrics to support a certain conception of a good live or the common good is morally illegitimate. It is up to the people to decide whether they want to use such technology to maintain their own utility.

Now, this seems to be the same answer as the one I have criticized at the beginning. Up till now I only made more clear why, from a libertarian and liberal point of view, the state and its agents are not entitled to interfere with the decisions of citizens to use or not to use technology in general and ICT implants or biometrics in particular. But as mentioned above, the use of such technologies often affects not only the person who wants to use it but others, too. Using ICT implants or biometrics for self-protection can, for instance, inherit illegitimate infringements into other persons’ private sphere. In such cases, there are two ways of solving collisions of rights and interests. The first one is favored by most libertarians: The person who infringes into the rights of others has to provide compensation to them – roughly speaking, she has to pay. However, in a complex world of uncountable interactions of people and technology that seems to be intractable. Therefore and because the state and its agents are obliged to protect citizens' rights, the second solution is that state authorities must prohibit the private use of such technology and, at the same time, must provide the protection that those persons seek who want to use π^3 technology – that is a necessary consequence of the state claiming the monopoly of power and force. Subsequently, the state is entitled and even obliged to use means like ICT implants and biometrics to protect its citizens against force, theft, and fraud, to enforce contracts, and the like. That leads to a libertarian and liberal paradox: *To protect civil rights of its citizens the state is entitled to reduce or even suspend these rights* – we all can learn the consequences of this paradox if we take a look on counter-measurements to fight terrorism.

5.2 Communitarian positions

On the one hand, utilitarian scholars argue that decisions shall be made in a way that the net utility in a society is maximized – communitarians, on the other side, stress that the common good is at stake. It would be interesting to see whether there is a difference in "net utility" and "common good" – from my point of view, there is none. But first things first. Amitai Etzioni, one of the most important communitarian scholars, argues in his book "The Limits of Privacy" (1999: 103/104) that

> "American society incurs high costs—social, economic, and other kinds—because of its inability to identify many hundreds of thousands of violent criminals, white-collar criminals, welfare and credit card cheats, parents who do not pay child support, and illegal immigrants. If individuals could be properly identified, public safety would be significantly enhanced and social and economic costs would be reduced significantly. […] We must hence ask:

> Do the benefits to public safety and other public goals of ID cards or biometrics outweigh the cost to privacy?"

Within the chapter on "ID Cards and Biometric Identifiers" Etzioni does not discuss ICT implants. However, with respect to privacy all his arguments could be applied to this technology, too. After the above cited passage, Etzioni presents a long list of problems that arise due to the non-existence of mandatory ID systems in the United States, for instance: criminal fugitives, child abuse, income tax fraud, illegal gun sales, illegal immigration, and identity theft.[5] After discussing some libertarian arguments against ID cards and the use of biometrics for a secure identification of a person he tries to reject those arguments from a communitarian point of view. Unfortunately, all points he makes are somehow technical: he stresses that, for instance, the abuse of ID cards could be handled, and so on, but there is no real ethical argument. But if one takes a closer look on communitarian arguments in general and adopt them to our issue, it is clear that communitarians would argue that the common good is prior to individual rights. First of all, they stress that "[…] the identity of the autonomous, self determining individual requires a social matrix, one for instance which through a series of practices recognizes the right to autonomous decision and which calls for the individual having a voice in deliberation about public action." (Taylor 1992: 209) Individuals are depending on society and the social resources it provides. Therefore "[…] the free individual who affirms himself as such *already* has an obligation to complete, restore, or sustain the society within which this identity is possible." (ibid.) Charles Taylor, and with him other communitarian scholars, emphasizes this point quite often (e.g. Taylor 1994: 59). From a communitarian point of view, that implies that we are obliged to maintain that society:

> "[…] we all approach our own circumstances as bearers of a particular social identity. I am someone's son or daughter, someone else's cousin or uncle; I am a citizen of this or that city, a member of this or that guild or

> profession; I belong to this clan, that tribe, this nation. Hence what is good for me had to be good for one who inhabits these roles. As such, I inherit from the past of my family, my city, my tribe, my nation, a variety of debts, inheritances, rightful expectations and obligations." (MacIntyre 1994: 124)

Regarding the law, libertarians would concede that citizens must obey it as long as it is a just law. However, in contrast to libertarians and liberals, communitarian scholars go further in their argumentation and claim that the state even is entitled to enforce a certain way of live:

> "Whereas liberals take the position that the state has to be *neutral* between the competing conceptions of the good, communitarians argue that the state ought to enforce that morality which is dominant within the community. […] Communitarianism […] gives the state the right to discriminate between different views of the good; the state is entitled to give special treatment to that morality which is dominant within the community." (Graf 1994: 141)

> „Whereas a liberal state will adhere to the *harm principle* and use the criminal system only against behaviour that harms other citizens, the communitarian state will outlaw harmless behaviour provided it contradicts the dominant morality.‟ (ibid.: 144)

In other words, communitarian and utilitarian argumentations are quite similar: a greater net utility respectively the common good and the protection of common morality justify sacrificing the rights of citizens. With regard to privacy the consequences are quite obvious. The state and its agents are entitled to use all their means and coercive power to support and enforce the common morality, the widespread conception of a common good, and citizens' support of both. This certainly includes ICT implants and biometrics as we can learn from Amitai Etzioni. *To protect the common morality and the widespread conception of a common good the state is entitled to reduce or even suspend civil rights like privacy.*

6. Final remarks

In this paper I tried to point out that if one argues that it is up to the people to decide whether and how to use ICT implants and biometrics that does not solve the important moral and social problems that could and certainly will arise by that use. Additionally, I tried to show that this vulgar libertarian as well as the contrary communitarian position that it is society's decision whether and how to use ICT implants and biometrics will lead to something like a "democratic Big Brother". We do not need a totalitarian state to fear that civil rights will fade away. It is important to see that ICT implants and biometrics are not the beginning of a process of evaporating civil rights like privacy but only another brick in the wall. Furthermore, it is vital to understand that this problem cannot be solved by other and new technology –civil rights protection is a social and political task and not one of engineers.

Let me end with two apercus and a somehow polemic question. The first apercu is a paraphrase of, as far as I remember, Mark Twain's Huck Finn: "If only one knows it, it is a secret. If two know it, it is no secret anymore. And if three know it, the whole world knows." The second apercu almost belongs to common knowledge. If one wants to prepare a revolution, a terrorist attack, or if one would like to build up a secret intelligence service then one rule strictly has to be followed: you must decide which persons shall have access to which information. After making that decision there must be no exception because it is too dangerous to distribute sensitive information among too many persons. Now, let us combine these two apercus. Using biometrics or ICT implants to identify persons anytime and anywhere inherits that too many people, state authorities, or even companies will know too much about us. There will be too many opportunities to use personal related information against us. That already provides good reasons to oppose ICT implants and biometrics as mandatory measurements to identify everybody anywhere.

But I said that I would like to finish with a polemic question. Here it is: Would a survivor of a Nazi concentration camp accept biometrics or ICT implants? I guess the answer is “no”. All inmates of Nazi concentration camps were tattooed. Of course, compared with current sophisticated ICT technology that is a quite primitive way to identify persons – but, unfortunately, it worked perfectly sixty years ago. A tattoo hardly can be removed; ICT implants are quite difficult to remove; biometrics cannot be removed at all without causing severe harm – of course you can throw away your eyes as shown in the motion picture “Minority Report”, but that is no real option. The possibility of identification anyone anytime everywhere may be no problem in a free society and a state ruled by the law. And of course, don’t get me wrong here, those who currently promote ICT implants and biometrics for identification purposes are not Nazis. However, we all know that societies and states can change completely and rapidly. Therefore, we should try not to willingly provide means to the state and its agents that make omnipresent control and suppression possible.

Notes

[1] This paper is the written version of presentation given at the ZiF Workshop on Privacy, February 10-11, 2006, Center for Interdisciplinary Research, University of Bielefeld, Germany.

[2] See, for instance, http://www.baja-beachclub.com/bajaes/asp/zonavip.aspx, http://www.prisonplanet.com/articles/april2004/040704bajabeachclub.htm, http://www.technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=104, last visit of all pages: 10-17-2006.

[3] One may say that this is somehow exaggerated. But even the rather low-tech of RFIDs that are implanted under the skin of beach club customers provides the possibility of comparable applications. RFID

technology could be used to track persons at the location; furthermore, it can be used to detect which persons often gather and which are staying alone. Even if one is unable to determine an application of such information that seems to make sense it is quite probable that marketing experts will create one.

[4] Particularly libertarians argue that rights are absolute constraints against infringements; with regard to civil rights I would like to mention that liberals agree to that position although it has to be stressed that there are important differences of libertarian and liberal positions, particularly regarding property rights and distribution of wealth. Therefore, I will discuss libertarian and liberal positions together, but one has to keep in mind that this only makes sense with regard to the issue of this paper.

[5] In publications on computer security, particularly identity theft is widely discussed with regard to biometrics (e.g. Grijpink 2004; Marshall, Tompsett 2005).

References

Barrera, M. H.; Okai, J. M. (1999): Digital Correspondence: Recreating Privacy Paradigms. In: International Journal of Communications Law and Policy, 3, http://www.ijclp.org/3_1999/ijclp_webdoc_4_3_1999.html, last visited 03-15-2005.

Berlin, I. (2002): Two Concepts of Liberty. In: Hardy, H. (ed.): Isaiah Berlin – Liberty. Oxford University Press: Oxford, New York, pp. 166-217.

Blythe, M.A.; Wright, P. C.; Monk, A. F. (2004): Little brother: could and should wearable computing technologies be applied to reducing older people’s fear of crime? In: Personal Ubiquitous Computing, 8, pp. 402–415.

Clarke, N. L.; Furnell, S. M. (2005): Authentication of users on mobile telephones – A survey of attitudes and practices. In: Computers & Security, 24, pp. 519-527.

Etzioni, A. (1999): The Limits of Privacy. New York: Basic Books.

Forte, D. (2003): Biometrics: Future Abuses. In: Computer Fraud & Security, 10, pp. 12-14.

Furnell, S. M.; Clarke, N. (2005): Biometrics: no silver bullets. In: Computer Fraud & Security, 8, pp. 9-14.

Furnell, S. M.; Dowland, P. S.; Illingworth, H. M.; Reynolds, P. L. (2000): Authentication and Supervision: A Survey of User Attitudes. In: Computers & Security, 19, pp. 529-539.

Graf, G. (1994): Contract Law and the Ethical Neutrality of the State: Some Thoughts about Liberalism and Communitarianism. In: Pauer-Studer, H. (ed.): Norms, Values, and Society. Dordrecht, Boston, London: Kluwer Academic Publishers, pp. 143-151.

Grijpink, J. (2004): Identity fraud as a challenge to the constitutional state. In: Computer Law & Security Report, 20 (1), pp. 29-36.

Leonhardt, U.; Magee, J. (1998): Security Considerations for a Distributed Location Service. In: Journal of Network and Systems Management, 6 (1), pp. 51-70.

Lyon, D. (2001): Facing the future: Seeking ethics for everyday surveillance. In: Ethics and Information Technology, 3, pp. 171–181.

MacIntyre, A. (1994): The Concept of a Tradition. In: Daly, M. (ed.): Communitarism. Belmont/California: Wadsworth Publishing Company, pp. 123-126.

Marshall, A. M.; Tompsett, B. C. (2005): Identity theft in an online world. In: Computer Law & Security Report, 21, pp. 128-137.

Narveson, J. (2001): Collective responsibility. In: The Journal of Ethics, Vol. 6, pp. 189-198.

Patton, J. W. (2000): Protecting privacy in public? Surveillance technologies and the value of public places. In: Ethics and Information Technology, 2, pp. 181–187.

Pecora, V. P. (2002): The Culture of Surveillance. In: Qualitative Sociology, Vol. 25, No. 3, pp. 345-358.

Prekop, P.; Burnett, M. (2003): Activities, context and ubiquitous computing. In: Computer Communications, 26, pp. 1168–1176.

Rawls, John (1999a): A Theory of Justice. Cambridge/Massachusetts: Harvard University Press, revised edition.

Rawls, J. (1999b): Justice as Fairness: Political not Metaphysical. In: John Rawls: Collected Papers. Cambridge/Massachusetts, London/England: Harvard University Press, pp. 388-414.

Raz, J. (1994): Ethics in the Public Domain. Oxford: Clarendon Press.

Taylor, Ch. (1992): Atomism. In: Kymlicka, W. (ed.): Justice in Political Philosophy, Volume II. Aldershot: Edward Elgar Publishing Ltd., pp. 337-360.

Taylor, Ch. (1994): The Modern Identity. In: Daly, M. (ed.): Communitarism. Belmont/California: Wadsworth Publishing Company, pp. 55-71.

Warwick, K. (2003): Cyborg morals, cyborg values, cyborg ethics. In: Ethics and Information Technology, 5, pp. 131-137.

Warwick, K.; Gasson, M. (2004): Practical Interface Experiments with Implant Technology. In: Sebe, N. et al. (eds.): Computer vision in human-computer interaction: ECCV 2004 Workshop on HCI. Prague, Czech Republic, May 16, 2004. Berlin et al.: Springer, pp. 7-16.

Wolff, J. (1991): Robert Nozick. Property, Justice and the Minimal State. Stanford/California: Stanford University Press.

Author's Biography

After vocational training in software engineering and a couple of years working as software engineer and system administrator, Karsten Weber (kweber@euv-frankfurt-o.de) studied Philosophy, Informatics, and Sociology at the University Karlsruhe, Germany. In 1999 he received his PhD in Philosophy. In the same year, he left Karlsruhe; since then, he is working at the European University Viadrina Frankfurt (Oder), Germany as researcher and lecturer for Philosophy. Since 2004, he is the head of the project “Mobile Internet Services and Privacy”, funded by the German Federal Ministry of Education and Research. Additionally, since the beginning of 2006, he is professor for Philosophy at the University Opole, Poland. Karsten Weber is co-editor of the online journal International Review of Information Ethics (http://www.i-r-i-e.net/). With regard to information and communication technology, he has authored a couple of papers about impacts of ICT on civil rights, about Open Source software, and about the digital divide. Together with Rafael Capurro, he was guest editor of CSI (Computer Society of India) Communications Issue “Information Ethics” in June 2006. In 2006 he translated the ACM and IEEE-CS Software Engineering Code of Ethics and Professional Practice (see http://seeri.etsu.edu/Ethics/Codes%20in%20PDF%20form/SEERI.Germancode.pdf).

Source: Ubiquity -- Volume 7, Issue 45 (November 21, 2006 November 27, 2006)

http://www.acm.org/ubiquity