# Chapter 6
# Information Ethics

## 6.1 Ethics of a New Culture

The knowledge society forms an entirely new culture. Knowledge is delinearized in and between hyperdocuments, graphic input devices (like the mouse) require less ability to write, while output links alphabetical signs with icons and graphics, thus changing the way we read. Computer and telecommunication are becoming uncircumventable tools. Knowledge is available everywhere, all the time. If this is indeed the case, then we are standing on the threshold from the culture of writing to the culture of multimedia. In taking this step, we would be entering the third phase of the informatization of human society, after the cultures of spoken language and of writing. Wolf Rauch (1998, 52) compares the current transition period with the move from spoken language to writing:

> A comparable cultural upheaval took place around 500 BC, in ancient Greece. Prior to this time, a culture of spoken language dominated in the Mediterranean region. … After that, only two generations, i.e. 50 to 60 years, were necessary in order to go from a predominantly speaking culture to a wide prevalence of writing culture.

A new culture requires new thinking about the values and norms that accompany such a "cultural earthquake" (Rauch, 1998, 55), and about which of the previous tenets should be adopted and which changed. Information ethics takes up this challenge: on the one hand, its objective is to think ahead to codified values (i.e. legal norms) (in places where no laws exist, as technical development moves a lot faster than legal) and to scrutinize existing regulations (in order to justify, but also to discard, where needed), and on the other hand, to work in areas beyond governmental standardization, which concern general ethical and moral subjects.

If we compare information ethics with (general) ethics, we can make the blanket statement that without information (no matter in what medial form), no ethics is possible in the first place, as moral action absolutely requires information streams. This is not the object, though. Rather, information ethics is a specific area

of ethics mainly concerning information. Luciano Floridi (1999, 43) describes this as follows:

> Without information there is no moral action, but information now moves from being necessary prerequisite for any morally responsible action to being its primary object.

Ethics–and thus information ethics–is purely descriptive on the one hand (observing how something *is*) as well as, on the other hand, normative (prescribing how something *should be*), as Rafael Capurro (2004, 6) observes:

> Information ethics can thus be conceived as a descriptive *and* emancipatory or normative theory, from a historical and systematic perspective, respectively:
>
> As a descriptive theory, it describes the different structures and power relations that determine information behavior in different cultures and eras.
>
> As an emancipatory or normative theory, it deals with the critique of the development of moral behavior in the area of information. It comprises individual, collective and human aspects.

Alongside the knowledge society, **power factors** arise, which must then be paid particular attention. Norbert Henrichs (1995, 34 et seq.) names the following examples:

> the power of chip manufacturers, from which all hardware producers depend (…);
>
> the power of the market leaders in the areas of hardware and software (…);
>
> the power of the providers of large (service) computer centers (…);
>
> the power of network providers and the providers of telecommunication services (…);
>
> the power of maintenance technicians (…);
>
> the power of database producers, providers and distributors (…);
>
> the power of those who are educated and authorized to use the systems.

Power always has to do with the possible abuse of or careless conduct with power. The position of power becomes particularly obvious if a company has a monopoly in a specific area (or is at least the predominant force), as is the case for Microsoft and PC operating systems, or Google and search engines. What virtues, which be-

haviors are morally justifiable in the information society, and which are not? We are in "virgin territory", in which "the condition of being human in itself is affected by the advances in informatization" (Henrichs, 1995, 36), and in which networking is regarded as "an art of living" (Capurro, 2003, 50). The information society demands its own information ethics. One of the tenets of an emancipatory information ethics could be, following Floridi (1999, 47):

> (I)nformation welfare ought to be promoted by extending (information quantity), improving (information quality) and enriching (information variety) the infosphere.

The subject areas of **ethics and law** are separated: in law, the central messages are "you may not / you must", whereas (normative) ethics states that "you should not / you should". Gerhard Reichmann (1998, 135) draws a clear line between law and ethics:

> Ethics … deals with socially desirable behavior, and from this, it derives–apart from those norms of behavior that are already subject of law–many behavioral guidelines which to obey is dictated by custom, reason and morals, but which to disregard entails no clearly defined negative consequences. In contrast to this, the law will ideally define required and forbidden behavior in a clear and binding fashion.

The goal of ethics can be to create justice (Rawls, 1971); the goal of information ethics would thus be, analogously, to establish "information justice" as the "utopian horizon" (Capurro, 2003, 84). The philosophical conceptions of morals and ethics (diverse as they are) try to justify human behavior in such a way that it is to be regarded as "good". One of the best-known formulations of moral law is by Immanuel Kant (1973[1788], 53):

> Act only according to that maxim whereby you can at the same time will that it should become a universal law.

Actions that follow this principle are morally good. Related to Kant's dictum is the "golden rule": do unto others as you would have others do unto you. If we were to relate Kant's "Categorical Imperative" to informational action, this would mean that one's own informational behavior is to be conducted in such a way that it should be–or, at the very least, could be–done in the same way, by everyone, always. One always has to ask oneself what the effects–on oneself, too–would be if one were to perform the action under consideration. If one detects problems for oneself, one must refrain from doing whatever one plans to do. An example from everyday life: if I do not want other people to "sniff around" on my site–let us say: on Facebook–without detection, I will not do so on other people's sites either.

What is the subject area of information ethics? According to John Weckert and Douglas Adeney (1997, IX), all areas of information processing are addressed:

> The domain of information ethics comprises all of the ethical issues related to the production, storage, access, and dissemination of information.

Information ethics is thus closely related to computer ethics. However, there are subjects in computer ethics–we need only think of the role of computers as "social agents" (Moore & Unsworth, 2005, 11)–that play no role in information ethics. On the other hand, subjects like fair knowledge representation, or access to public libraries for all members of society, are hardly of interest for computer ethics.

Information ethics is thus exclusively distinguished from ethics in general via its reference to information activity as restricted above. Although information ethics is as a professional ethics (i.e. an ethics regarding a certain profession–information scientists and related jobs), most of its questions are of such a universal nature that they regard everybody living in an information society.

Apart from professional information ethics, the following three subject areas are relevant for an ethics of the knowledge society (for a comprehensive bibliography, cf. Carbo & Smith, 2008): Free access to information, protection of privacy and the question of who own knowledge (Figure 6.1). These subjects are interlinked and may even work in opposite directions. Thus, free access to knowledge will find its limits in the definition of privacy. Or, in other words: if a certain information represents intellectual property, they cannot be used freely.

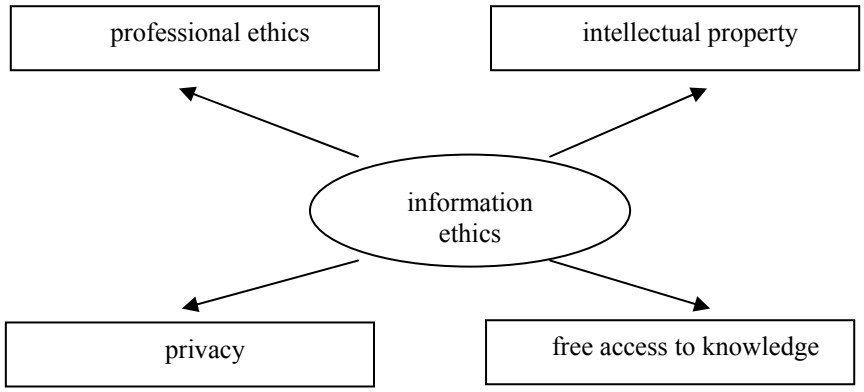


*Figure 6.1: Subject Areas of Information Ethics.*

## 6.2 Professional Behavior

The aspect of professional information ethics (Weckert & Adeney, 1997, 17 et seq.) becomes particularly clear in the case of "professional guidelines", or "codes of ethics", as brought forward by many information-professional associations, e.g. the Association for Computing Machinery (ACM, 1992), the American Library Association (ALA, 2008) and the American Society for Information Science & Technology (ASIS&T, 1992). They regulate the professional behavior of computer scientists, librarians and information scientists by stipulating norms that their members should adhere to.

According to Froehlich (1992), the professional is in an eternal triangle between his self, his organization and the respective context; he avoids unethical behavior and acts courageously in the sense of his moral guidelines (Hauptman, 2002).

A professional information ethics can include, for example, the maxims of a fair knowledge representation to not exclude any relevant sources in digital information services or index or refer to topics in a malicious manner. Likewise, information professional are required to keep secret any information pertaining to their employers (including the enquiry topics) in the context of conducting a research or creating information profiles. Scientific authors, for instance, are asked to cite, according to their best knowledge, everything they have read and used in the preparation or completion of a publication, and furthermore, only to appear as author if they have actively contributed to the publication of a text (avoiding "ghostwriting" and "honorary authorships") (Fröhlich, 2006).

## 6.3 Free Access to Knowledge

There is a lot of demand for free access to knowledge. The ethical question in this context is: what knowledge should be freely available to whom? Not all information should be freely available, evidently: trade secrets should stay in the business, delicate, person-related information with their carrier and false information that would humiliate and insult certain people should not even be created in the first place. Also, "free" cannot always be taken to mean "free of charge". Commercial information–let us say: market research reports–are free in the sense that anybody can acquire them in principle, but they are not free of charge; generally, they are sold in the high-price range.

Private knowledge goods (such as the content of a patent-protected invention) or mixed goods (such as the content in digital databases) are protected via laws (copyright and commercial legal protection). The rights holder thus has a large influence on the kind of access that is possible to such information. (The ethical problems of intellectual property will be discussed further below)

If free access to information is guaranteed by the constitution, as it is in Germany (in Section 5 of German Basic Law), the onus is on the government. Free

access to public **libraries** is clear. The American Library Association's "code of ethics" (ALA, 2008, I) has the following perspective:

> We [the librarians] provide the highest level of service to all library users through appropriate and usefully organized resources; equitable service policies; equitable access; and accurate, unbiased, and courteous responses to all requests.

This goes for all actual library visits, but also for any availment of library information services via digital channels, such as e-mail, chat or forms on the WWW (Hill & Johnson, 2004).

The question of whether it is the government's duty to digitally compile information (at least for important areas of life, such as health, education or law) and distribute it is still under debate (Capurro, 1988). For the public sector, this means financing the production of **electronic spezialized information** as well as its distribution via search engines or online archives. Several countries (such as the U.S.A.) assume this burden and finance the corresponding information services in the context of universal services (even going so far as to distribute the results for free), many others (including Germany) keep a low profile and only subsidize information providers if they compile information for federal ministries (as in the case of the DIMDI) or if they manage important STM information in the context of the principle of subsidiarity (as in the case of the FIZ Karlsruhe).

The norm of **communication freedom** (the right for free communication) can be separated into two subnorms: the right to read and the right to write. According to Rainer Kuhlen (2004, 262), information ethics specifies a regulative idea

> of keeping communicative spaces as open and permissive as possible, so as not to restrict any developmental freedoms via containment strategies.

Censorship is the active prevention of the distribution of content, independently of the respective carrier. Censorship can thus apply to books, newspaper articles, films or content on the World Wide Web. Censorship is the counterpart to freedom of expression and to free access to information. An indisputable limit of freedom of expression is its interference with other people, e.g. when person-related information is published or people are defamed or slandered. Weckert and Adeney (1997, 47) emphasize:

> The freedom of expression of one person can cause harm or offence or both to another, so some restrictions need to be placed on how and to what extent a person can be allowed free expression.

While not taking into account this (very weak form of) "censorship", there are five subject areas for which censorship is under serious discussion (the first four after Weckert & Adeney 1997, 51 et seq.):

- pornography (e.g. sex with animals, sex with minors),
- hateful content (e.g. racism),
- information supporting criminal or terrorist activities (e.g. instructions for building a suitcase bomb),
- "virtual violence" (e.g. the gruesome execution of a character in a digital world),
- contents that are in opposition to an (accepted) opinion (e.g. anti-Islamic representations, anti-semitism, content attacking China).

Censorship occurs in all five forms, all of which are protected by corresponding laws in certain countries. Censorship is expressed (as is the case in Germany, for pornographic documents displaying sex with minors) by penalizing the possession of censored documents, blocking certain websites with hateful content from being registered by search engines (again, in Germany, the deletion of indexed information about fascist literature on Google.de) or blocking undesirable content via large-scale national firewalls (as is currently the case in China).

It may be possible to find justification for single forms of censorship, but it is very difficult by principle to draw a clear, unarbitrary line between permissible and inadmissible content. Due to the "side effects", it seems ethically reasonable to generally reject censorship on the internet (with the sole exception of damage to specific persons, including representations of sex with children). Weckert and Adeney (1997, 55) arrive at the following result for the assessment of the pros and cons of censorship:

> Effectively censoring activity on the Internet will not be easy to do without limiting its usefulness. While it may not be good that certain sorts of things are communicated, ... it may well be worse overall if this form of communication is restricted in ways that would limit the effectiveness of the Internet. It is difficult to see how it would be possible, given current technology, not to throw out too many babies with the bath water.

Free access to information and communication freedom are fundamental rights of every person, and not merely of an intellectual or economic elite. Jack Balkin (2005, 331 et seq.) expresses this very pointedly on the subject of digital communication in a democratic culture:

> Freedom of speech is more than the freedom of elites and concentrated economic enterprises to funnel media products for passive reception by a docile audience. Freedom of speech is more than the choice of which media products to consume. Freedom of speech means giving everyone–not just a small number of people who own dominant modes of

> mass communication, but ordinary people, too–the chance to use technology to participate in their culture, to interact, to create, to build, to route around and glom on, to take from the old and produce the new, and to talk about whatever they want to talk about, whether it be politics, public issues, or popular culture.

For all those who have access to the internet and know how to use the technical means that can be found there, its services (we need only think of weblogs and search engines) provide new possibilities for optimizing both freedom of communication and free access to information. However, the new information services also carry problems with them (Balking, 2005, 341):

> However, these same technological changes also create new forms of social conflicts, as business interests try to protect new forms of capital investment.

Thus it is definitely rational economic behavior if a search engine that generates profits via advertising also wants to do business in a country that censors certain information. Correspondingly, this business–in order to take up the above example of Google once more–will adjust to the respective government guidelines and make parts of its database inaccessible for users from that country. The index for both the German and Chinese versions of Google is censored at the time. These conflicting goals between economic and ethical interests should continue to exist in the knowledge society.

## 6.4 Privacy

Respect of privacy is mentioned explicitly in all of the professional information ethics we cited (ACM, 1992, 1.7; ALA, 2008, III; ASIS&T, 1992). The subject of privacy touches on many problems that people deal with in their attitude toward information technology (Weckert & Adeney, 1997, 75).

> People are worried about the ease of the collection of personal data, its large-scale storage and easy retrieval, and about who can get access to it. They are also worried about the surveillance made easy by computer systems.

Privacy is one of the counterweights to free access to information. If people were at a disadvantage due to free access to "their" information, that information should not be freely available. Above, we called this a "weak form" of censorship. However, privacy can definitely be regarded as a human right (Kerr & Gilbert, 2004, 171):

> Our right to privacy is a fundamental human right, one that allows us to define our individuality free from interference by the state and its agents.

We would like to distinguish between ongoing person-related information and traces that an individual leaves behind in digital spaces. Among the first group of privacy information are demographic statements (age, gender, job, income etc.), health information (from the digital patient file), bank connections (including PIN code) etc.

The second group of privacy information is made up of **digital traces** (Kuhlen, 2004, 186 et seq.), which may consist of an Internet Service Provider (ISP) or search engine collecting data and allocating it unequivocally to a person (or an internet address, or a password). If a public authority gains access to these traces, ISPs act "as agents of the state" (Kerr & Gilbert, 2004, 166). The data provided others–let us say: prosecuting authorities–by Internet Service Providers as well as other internet agencies concern four levels:

- customer names and their addresses,
- "traffic" data: e-mail (sender, recipient, subject, extent) or Web (URLs visited),
- content (e.g. e-mail text, search arguments in search engines),
- transactions (products bought, financial transactions).

A particular technique of securing digital traces is epitomized by **spyware** (Stafford, 2008, 619):

> Spyware is a class of remote monitoring applications designed to survey and report across the Internet to third parties about computer user behavior.

Spyware is not always ethically problematic. The URLs accessed by users of a toolbar provided by a Web service, for instance, are transmitted to the service provider and then–in anonymous form–generate data for Relevance Ranking. However, if a user has not given his consent to such actions, if the statements are not anonymous or if the spyware takes over the computer's capacity for criminal purposes (as in the creation of a botnet), massive legal and moral concerns arise.

If we take seriously the human right to privacy, data from all levels fall under privacy and may not be transmitted for private, commercial or public purposes due to ethical reasons. However, if ISPs are only required by law to save data, and copy it by request, they will not be able to say not. Especially the more elaborate tools of information science–such as retrieval systems–pave the way toward the gapless surveillance of contents, be it online, in e-mail traffic or for the scouring of private computers for content. Retrieval research and practice can, without a doubt, work out algorithms that make the content of e-mails searchable, but the question is whether it should. If governmental regulations threaten aspects of pri-

vacy (e.g. the U.S. "Patriot Act"), it must be considered whether the loss of privacy (to be deemed a negative aspect) is made up for by the protection of society from criminal or terrorist activity (positive) (Lilly, 2005). According to Rainer Kuhlen (2004, 195), the object is

> to maintain the balance between the justified demand for security and the right for privacy and informational self-determination. … The ambivalence is clear: there will be no privacy if security is not safeguarded. However, security is worthless if there is no more privacy, or if it is too restricted.

Search engine providers evaluate search arguments and accessed websites gleaned from personalized access in order to adjust the retrieval service to each individual user, thus optimizing it. E-commerce companies save their customers' transaction information in order to be able to use it in the context of recommender systems–also for the user's benefit. In Customer Relationship Management, it becomes possible to pointedly address the individual customer (Gurau, 2008). Collaborative services in Web 2.0 evaluate user information in order to bring together users with similar interests into a community. All these services are only made possible by the consequent tracing of person-related information. In many cases, the resulting services–optimized research, specific product recommendations, communities–are useful for the persons concerned, if not expected (particularly in Web 2.0).

The collection of person-related data–by government authorities as well as the private sector–is reminiscent of George Orwell's *Nineteen Eighty-Four* (Severson, 1997, 73 et seq.):

> If "Big Brother" denied us all personal privacy, our self-identities would be destroyed just as Winston Smith's was in Orwell's *Nineteen Eighty-Four*. Privacy is one of the necessary ingredients of self-identity.

The least we can expect from services that deal with person-related data and traces is, according to Severson (1997, 74):

> (1) that they get permission before using private information for secondary purposes; and (2) that they provide people with free opportunities to correct inaccuracies in their records.

If a person knows or suspects that their privacy is being invaded, the result is an interesting specific moral problem: is it justified to lie under such conditions (Al-Fedaghi, 2005)? **Lying** can mean, in this case, making false person-related statements, but it can also consist of knowingly generating entirely senseless search terms (in case of suspected surveillance), entering invalid URLs etc., in order to obscure one's actual behavior via static. Is the person-related information of an

individual their (intellectual) property, which only they can decide how to use (Moore, 2005)?

Securing privacy means, in the end, acting discreetly–even in digital space. **Discretion** is regarded as a "virtue of the information age" (Nagenborg, 2001, 123), both for public authorities and for the internet's private users. Everybody should stand behind the things they reveal of themselves; nobody, though, should make private information about others public (at least not without their consent), or acquire such information in an untoward manner (e.g. via tracing on the internet). According to Michael Nagenborg (2001, 124) the following holds for the individual:

> We must learn to adequately disengage from the internet if we want to create something like privacy.

Discretion does not mean turning a blind eye to illegal action–on the contrary. Nagenborg (2001, 124) states:

> Discretion must not be confused with arrogance. Illegitimate information (e.g. incitement to criminal acts) must be reacted to in the same manner as in the urban public.

To clarify, Helmut F. Spinner (2001, 28) introduces the concept of "information encroachment". This is an analogous construct to "normal" encroachment, such as murder or assault.

> Knowledge can cause harm in other ways, which are often of no less consequence and possibly even harder to heal. Private confrontation and political struggle strike wounds; confessions are often embarrassing; denunciations are nefarious … .

Information encroachment can be imperative (in the case of the digital observation of a crime), but in most cases, it is forbidden (Spinner, 2001, 30):

> A case of information encroachment that is to be forbidden in any case is one that concerns the publication of false, misleading or exaggerated information *that causes harm to others* or, conversely, the concealment of true facts, as is the case in everyday insults, libel, defamation, breach of secrecy … etc.

"Informational self-determination", then, is the defense from "heteronomy by information encroachment" (Spinner 2001, 86)–a conception that goes far beyond codified data protection. Informational self-determination also means that every

person must be informed about every kind of information encroachment and have the possibility to either delete or correct information regarding themselves, and know, furthermore, "to what extent and under what conditions (others) may use this knowledge" (Kuhlen, 2004, 189).

Privacy means the privacy of *one* person. But what if one individual has built up several "identities" in different digital spaces? Different names (e.g. for chatting) and **avatars** are not unusual. Stephan Werner (2003, 103-104) compares avatars and aliases with puppets:

> (T)he chosen chat name can be regarded as an agent of the individual. It appears as an autonomous (virtual) object, which can be clearly identified and, in consequence, has its own identity with its own specific attributes that are not the individual's. The relationship between it and the individual can thus be likened to a puppet's relationship to its puppeteer. "Virtual Identity" is thus the identity of the software agent, who in this instance serves as the individual's proxy.

Similarly to a puppet, though, the avatar/alias is as legally incompetent in e-commerce as it has no just claim on "its" intellectual property, as these characteristics are only "its" individual's. according to Werner (2003, 110), people are thus granted a "chance for individuality", in the positive sense (which can be, on the other hand, a pathological "chance" at schizophrenically splitting up one's personality); in the negative sense, this "encompasses a lack of reliability in social relationships" (Werner, 2003, 110). Avatars (or computer systems) are not the subject of information ethics–information ethics is always aimed at people, or–as Bernd Frohmann (2002, 50) expresses it:

> I argue that cyberethics has to do with bodies, not bytes.

## 6.5 Intellectual Property

Intellectual property is owning an intangible, ideal object, such as an invention or a work of art. In information law, the protection of intellectual property comprises copyright as well as commercial legal protection (regarding patents, utility models, brands and designs). Professional information ethics come out in favor of protecting intellectual property. In the ACM (1992, 1.5; 1.6), we read:

> [As an ACM member, I will ...] (h)onour property rights including copyright and patents; (g)ive proper credit for intellectual property.

This is also obvious for the American Library Association (ALA, 2008, IV):

> We respect intellectual property rights and advocate balance between the interests of information users and right holders.

Western societies have been protecting intellectual property for centuries; the reasons behind this are largely economic in nature. Richard W. Severson (1997, 32) emphasizes:

> Since the Middle Ages, Western societies have attempted to protect intellectual property rights through legal means. The primary mechanisms for such protection are trade secrecy, copyright, and patent laws. The legal protection of intellectual property has always been commercially motivated.

If a small company produces a groundbreaking invention and wants to exploit it by itself, it requires a protective mechanism, since otherwise, large companies could take up this invention immediately after its release to the public and, due to their market power, be able to exploit it much more effectively than its inventor. Commercial protective rights grant our small company a monopoly on using its innovation, at least for a certain period of time. Without such protective rights, there would hardly be any reason for freelance inventors as well as small to mid-size companies to even go into research and development at all. This **utilitarian argument** for intellectual property protection (Palmer, 1997) emphasizes the value for all members of society, which would not be given without such protective mechanisms. The value argument is double-edged, though, since it is perfectly possible to claim (and possibly to prove) that it is always more beneficial to a society if intellectual works belong to nobody, being everyone's property "in the public interest".

Apart from utilitarianism, there are three further lines of argument that speak in favor of intellectual property protection. (1.) Works are the expression of individuals' **efforts**. Without legal protection, they would be deprived of the fruits of their labor. If someone develops, designs or discovers something new, he deserves protective authorship rights. Tom Palmer (2005, 131) expresses this as follows:

> When one has improved what was before unimproved (or created what before did not exist), one is entitled to the results of one's labor. One deserves it.

(2.) The works of a creator are an expression and a part of his **personality**. Without protection, it would hardly be possible for the author to take responsibility for his works, because in that case, they would not belong to him (Palmer, 2005, 143):

> In fact, the relationship between creator and creation is so intimate that when the personality of the former changes, so too can the treatment of the latter.

This becomes particularly clear in the case of a work of visual art: the destruction of a painting does indeed affect the personality of the artist. At this point, we have to stop and ask ourselves what a "work" is, since it is the only concept that is so closely tied to the person of its creator. According to the IFLA (1998), we distinguish between two aspects of a document's content ("work" and "expression") as well as two aspects of its physical form ("manifestation" and "item"). The work is the author's creation, which is concretely realized as an "expression" (e.g. as an illustrated book or a translation into a foreign language). The manifestation is effectively the "embodiment" of an "expression", it is a certain edition with special characteristics (e.g. a softcover book). The item, finally, is the concrete book of a manifestation. If you, dear reader, think that the book you are in the process of reading is "your" book (i.e. your property), what you mean is that the item in question is yours. If we, as its authors, claim that it is "our" book (and thus our property), we are not contradicting you, since we refer to the level of the work. The discussion about intellectual property always revolves around works. Thus authors are the owners of their works, whereas translators are not the owners of the translated text (we are now on the level of "expressions"); the translation, too, remains the authors' intellectual property.

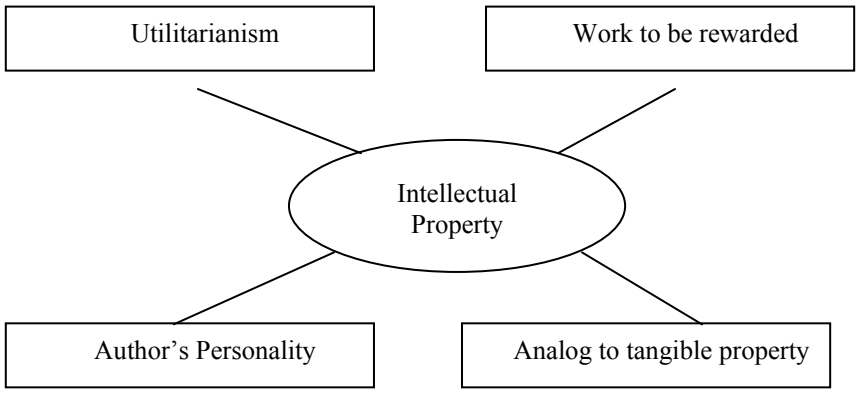


*Figure 6.2: Lines of Argument for the Protection of Intellectual Property.*

(3.) Ownership of intangible goods is nothing other than **"normal" ownership** of a tangible good. Just as a person owns a piece of land or a house, the Coca-Cola Company–to take a random example–owns the formula for its drink (which, by

the way, was never patent-protected–such a patent would have long since run out– but has been and always will be a company secret) (Palmer, 2005, 150):

> If a chemist for the Coca-Cola company were to reproduce the formula for Coca-Cola (...) on leaflets and drop them over New York, the Coca-Cola company would have uncontestable grounds for (drastic) legal action against the violator of their secret and any of his conspirators.

The damage for Coca-Cola would be gigantic, since anyone who would find such a leaflet, read and understand the formula and then use it in his own soft-drink company cannot be legally tried (as there is no patent). In such cases, intellectual property must be treated in the same way as any other property. Palmer (2005, 149) calls this line of argument "piggybacking", as intellectual property is basically carried into legal protection on the back of normal ownership rights. Figure 6.2 charts the four theories defending ownership rights for intangible goods.

Intellectual property is a **privilege** of the owner (Palmer, 2005, 126) to dispose of his property at his guise. But is such private ownership of ideal objects really that unproblematic, ethically speaking? To whom does knowledge belong (Kuhlen, 2004, 311 et seq.)? Let us consider the case of an online research. The researcher has bought a certain amount of data sets from a provider of digital information and downloaded them onto his computer. He now wants to send the result of his research to a colleague via e-mail, i.e. make a digital copy of it. The provider DIALOG states, in its General Terms and Conditions:

> Under no circumstances may Customer, or any party acting by or through Customer, copy, transmit or retain data retrieved from DIALOG service in machine-readable form.

Our researcher is thus prohibited from digitally transmitting his (paid-for) research result. Is this ethically sound? Weckert and Adeney (1997, 68) initially defend payment for content with regard to the value provided by a company such as DIALOG:

> Having databases is useful. They are expensive to build and maintain. Unless the vendors get a reasonable return for their efforts, there will be no databases. Given the structure of our society, they must make their profit from the users, so users must pay for the service.

On the other hand, prohibiting the transmitting of the information thus gleaned is not ethically defendable, since no (notable) economic damage is to be expected by the company as a result of it (Weckert & Adeney, 1997, 69):

> People generally undertake online searching to find material on some particular interest of theirs. It is unlikely that many others will want just

> those specific results, so it is hard to see that profits would be much affected. Thus we have no good reasons for the restrictions that are in place on online search results.

Now we will slightly tweak our example. Let us assume digital full texts of scientific articles, and the practice of inter-library loans. Now, one single library in all of Germany has subscribed to this particular journal. The others, who have not, will order single articles via inter-library loan, by individual requests from users. As in the above DIALOG example, digital copies of a journal (already paid-for) are transmitted. Here, though, the publisher must expect considerable economic damage. If only one single subscription (at "normal" prices, and not under consortium or national licenses, which let publishers break even) is made per country (or per library network), the publisher will not recoup its expenses (and as a consequence, have to cancel the magazine). This, in turn, is not only a disadvantage for the publisher, but also for the scientific community in question. In this second case (which is precluded by German copyright law), the transmission of information is not ethically defensible.

From an ethical perspective, the first example represents a **fair use** of intellectual property, whereas the second one does not. This "fair use", seems to be one of the keys for dealing with intellectual property (Severson, 1997, 50-51):

> Fair-use doctrine protects the often overlooked societal aspects of copyright law by ensuring the right of researchers, teachers, and ordinary citizens to use copyrighted materials freely for specific purposes. ... Suppose you want to read a magazine article at the public library. You could sit down and read it there, or you could make a photocopy and take it home to read later. Under fair-use guidelines, it is acceptable to photocopy articles–even books–if the photocopy is for temporary personal use. On the other hand, it would not be acceptable to make ten copies and distribute them at your PTA meeting.

"Fair" also means asking **fair prices** for information goods. If members of certain (poor) countries or (poor) social groups are unable to pay the asking price for information on the sole basis of their economic situation, they will be excluded from free access to knowledge. "Fair" may mean, in this context, to layer prices in a group-specific manner, i.e. to offer different prices for citizens of developing countries and those of the First World, or for the economic elite and the socially underprivileged (Ponelis, 2007, 5).

**Crawling** the Web consists of searching, copying, indexing and saving websites for use in search engines. There is no question of respecting ownership rights. Thelwall and Stuart (2006, 1775) observe:

> Crawlers ostensibly do something illegal: They make permanent copies of copyright material (Web pages) without the owner's permission.

This practice is particularly delicate in the case of the Internet Archive (archive.org), as it saves "historic" websites, and thus occasionally those that have been consciously overwritten or deleted by the owner of this intellectual property. Search engines such as the Internet Archive refer to the Robots.txt protocol, in which website owners give crawlers instructions for dealing with their site (e.g. NOINDEX or NOFOLLOW). Also, site owners are allowed to request deletion by the Archive. The practice of search engines to copy everything not explicitly excluded in Robots.txt, and to remove only when asked to, seems to be widely tolerated (and can–as it is in the U.S.A.–be regarded as "fair use"). As far as the sites contain information that can be abused (e.g. e-mail addresses for sending spam), this practice definitely has its disadvantages for users and is, ethically or even legally speaking, at least problematic. Evidently, it is regarded as extremely desirable at the moment or a crawler to illegally copy websites that are technically protected by copyright, following the principle "Esse est indicato in Google" (Hinman, 2005).

What about the legal protection of intellectual property in the case of collaboratively created software and content (such as Wikipedia)? According to Lawrence M. Sanger (2005, 193), this is a case of **shopwork** ("*sh*ared *op*en *work*"). Shopwork has two main characteristics: such works are freely available (open source, open content), and they have been created in strict collaboration. If collaboratively created software and collaboratively created content are important for a society (as is often claimed), the society in question must take responsibility for the ability of the creators of software and content to be able to make a living from their work, which is obviously valuable. This does not lead to a new copyright for shopwork, but instead to the (pretty extreme) ethical maxim of sufficiently financing the authors (Sanger, 2005, 200):

> (T)he law should actually *support* such works, either through funding or other special legislative support.

For Milton Mueller (2008), there is no contradiction between knowledge regarded as property (**information capitalism**) and publicly accessible knowledge (**information communism**). Especially on the internet, both forms of dealing with knowledge can co-exist without a problem: commercially distributed software or commercially distributed content (protected by commercial property rights) is pitted against free software and free content (only protected via Creative Commons, for example). According to Mueller (2008), the challenge is in finding the "right" application for both approaches:

> One could even argue that the success of liberal-democratic governance hinges on finding the right place for each model and exploiting the creative relationship between the two.

It is thus ethically justifiable to rate the author's right to his work more highly than the right of all others to access to this knowledge (Himma, 2008, 1160). This in no way excludes the possibility of the author deliberately waiving some of his rights and making his work publicly accessible. If a country wants to strengthen authors– even economically–they must create an artificial shortage (as for tangible goods) for knowledge goods (here via commercial property rights) (Palmer, 2005, 157):

> Tangible goods are clearly scarce in that there are conflicting uses. It is that scarcity that gives rise to property rights. Intellectual property rights, however, do not rest on a natural scarcity of goods, but on "artificial, self-created scarcity". That is to say, legislation or legal fiat limits the use of ideal objects in such a way as to create an artificial scarcity that, it is hoped, will generate greater revenues for innovators.

## 6.6 Conclusion

Only available in the printed version.

## 6.7 Bibliography

ACM (1992). ACM Code of Ethics and Professional Conduct.

ALA (2008). Code of Ethics of the American Library Association.

Al-Fedaghi, S. (2005). Lying about private information: An ethical justification. Communications of the International Information Management Association, 5(3), 47-56.

ASIS&T (1992). ASIS&T Professional Guidelines.

Balkin, J.M. (2005). Digital speech and democratic culture: A theory of freedom of expression for the information society. In Moore, A.D. (ed.), Information Ethics. Privacy, Property, and Power (pp. 297-354). Seattle, London: University of Washington Press.

Capurro, R. (1988). Informationsethos und Informationsethik–Gedanken zum verantwortungsvollen Handeln im Bereich der Fachinformation. Nachrichten für Dokumentation, 39, 1-4.

Capurro, R. (2003). Ethik im Netz. Wiesbaden: Steiner.

Capurro, R. (2004). Informationsethik–eine Standortbestimmung. International Journal of Information Ethics, 1, 1-7.

Carbo, T., & Smith, M.M. (2008). Global information ethics: Intercultural perspectives on past and future research. Journal of the American Society for Information Science and Technology, 59(7), 1111-1123.

Floridi, L. (1999). Information ethics: On the philosophical foundations of computer ethics. Ethics and Information Technology, 1, 37-56.

Fröhlich, G. (2006). Plagiate und unethische Autorenschaften. Information–Wissenschaft und Praxis, 57, 81-89.

Froehlich, T.J. (1992). Ethical considerations of information professionals. Annual Review of Information Science and Technology, 27, 291-324.

Frohmann, B. (2002). Cyberethik: Bodies oder Bytes? In Hausmanninger, T., & Capurro, R. (eds.), Netzethik. Grundlegungsfragen der Internetethik (pp. 49-58). München: Fink.

Gurau, C. (2008). Privacy and online data collection. In Quigley, M. (ed.), Encyclopedia of Information Ethics and Security (pp. 542-548). Hershey, PA: Information Science Reference.

Hauptman, R. (2002). Ethics and Librarianship. Jefferson, NC, London: McFarland.

Henrichs, N. (1995). Menschsein im Informationszeitalter. In Capurro, R., Wiederling, K., & Brellochs, A. (eds.), Informationsethik (pp. 23-36). Konstanz: UVK .

Hill, J.B., & Johnson, E.W. (2004). Ethical issues in digital reference. In Mendina, T., & Britz, J.J. (eds.), Information Ethics in the Electronic Age (pp. 99-106). Jefferson, NC, London: McFarland.

Himma, K.E. (2008). The justification of intellectual property: Contemporary philosophical disputes. Journal of the American Society for Information Science and Technology, 59(7), 1143-1161.

Hinman, L.M. (2005). Esse est indicato in Google: Ethical and political issues in search engines. International Review of Information Ethics, 3, 19-25.

IFLA (1998). Funetional Requirements for Bibliographie Records. München: Saur.

Kant, I. (1985[1788]). Critique of Practical Reason. New York, NY, London: Macmillan. (Original: 1788).

Kerr, I., & Gilbert, D. (2004). The role of ISPs in the investigation of cybercrime. In Mendina, T., & Britz, J.J. (eds.), Information Ethics in the Electronic Age (pp. 163-172). Jefferson, NC, London: McFarland.

Kuhlen, R. (2004). Informationsethik. Umgang mit Wissen und Information in elektronischen Räumen. Konstanz: UVK.

Lilly, J.R. (2005). National security at what price? A look into civil liberty concerns in the information age under the USA Patriot Act. In Moore, A.D. (ed.), Information Ethics. Privacy, Property, and Power (pp. 417-441). Seattle, WA, London: University of Washington Press.

Moore, A.D. (2005). Intangible property: Privacy, power, and information control. In Moore, A.D. (ed.), Information Ethics. Privacy, Property, and Power (pp. 172-190). Seattle, WA, London: University of Washington Press.

Moore, A.D., & Unsworth, K. (2005). Introduction. In Moore, A.D. (ed.), Information Ethics. Privacy, Property, and Power (pp. 11-28). Seattle, WA, London: University of Washington Press.

Mueller, M. (2008). Info-communism? Ownership and freedom in the digital economy. First Monday, 13(4).

Nagenborg, M. (2001). Diskretion in offenen Netzen. IuK-Handlungen und die Grenze zwischen dem Privaten und Öffentlichen. In Spinner, H.F., Nagenborg, M., & Weber, K. (eds.): Bausteine zu einer Informationsethik (pp. 93-128). Berlin, Wien: Philo.

Palmer, T.G. (1997). Intellectual property rights: A non-Posnerian law and economics approach. In Moore, A.D. (ed.), Intellectual Property: Moral, Legal, and International Dilemmas (pp. 179-224). New York, NY: Rowman & Littlefield.

Palmer, T.G. (2005). Are patents and copyrights morally justified? The philosophy of property rights and ideal objects. In Moore, A.D. (ed.), Information Ethics. Privacy, Property, and Power (pp. 123-168). Seattle, WA, London: University of Washington Press.

Ponelis, S.R. (2007). Implications of social justice for the pricing of information goods. International Review of Information Ethics, 7, 1-5.

Rauch, W. (1998). Informationsethik. Die Fragestellung aus der Sicht der Informationswissenschaft. In Kolb, A., Esterbauer, R., & Ruckenbauer, H.W. (eds.), Cyberethik. Verantwortung in der digital vernetzten Welt (pp. 51-57). Stuttgart, Berlin, Köln: Kohlhammer.

Rawls, J. (1971). A Theory of Justice. Cambridge, MA: Harvard Univ. Press.

Reichmann, G. (1998). Informationsrecht in Österreich. In Kolb, A., Esterbauer, R., Ruckenbauer, H.W. (eds.), Cyberethik. Verantwortung in der digital vernetzten Welt (pp. 135-152). Stuttgart, Berlin, Köln: Kohlhammer.

Sanger, L.M. (2005). Why collaborative free works should be protected by the law. In Moore, A.D. (ed.), Information Ethics. Privacy, Property, and Power (pp. 191-206). Seattle, WA, London: University of Washington Press.

Severson, R.W. (1997). The Principles of Information Ethics. Armonk, NY, London: Sharpe.

Smith, M.M. (1997). Information ethics. Annual Review of Information Science and Technology, 32, 339-366.

Smith, M.M. (2001). Information ethics. Advances in Librarianship, 25, 29-66.

Spinner, H.F. (2001). Was ist ein Informationseingriff und was kann man dagegen tun? In Spinner, H.F., Nagenborg, M., & Weber, K.: Bausteine zu einer Informationsethik (pp. 11-91). Berlin, Wien: Philo.

Stafford, T.F. (2008). Spyware. In Quigley, M. (ed.), Encyclopedia of Information Ethics and Security (pp. 616-621). Hershey, PA: Information Science Reference.

Thelwall, M., & Stuart, D. (2006). Web crawling ethics revisited: Cost, privacy, and denial of service. Journal of the American Society for Information Science and Technology, 57(13), 1771-1779.

Weckert, J., & Adeney, D. (1997). Computer and Information Ethics. Westport, Conn., London: Greenwood.

Werner, S. (2003). Aspekte der Individualität im Internet. In Hausmanninger, T. (ed.). Handeln im Netz. Bereichsethiken und Jugendschutz im Internet (pp. 95-112). München: Fink.