This is a preprint version of the following article:
Brey, P. (2007), "Ethical Aspects of Information Security and Privacy", in: *Security, Privacy, and Trust in Modern Data Management*, M. Petković and W. Jonker (Eds.), Springer Berlin Heidelberg, pp. 21-36.

Ethical Aspects of Information Security and Privacy

Summary. This essay reviews ethical aspects of computer and information security and privacy. After an introduction of ethical approaches to information technology, the focus is first on ethical aspects of computer security. These include the moral importance of computer security, the relation between computer security and national security, the morality of hacking and computer crime, the nature of cyberterrorism and information warfare, and the moral responsibilities of information security professionals. Privacy is discussed next. After a discussion of the moral importance of privacy and the impact of information technology on privacy, privacy issues in various information processing practices are reviewed. A concluding section ties the two topics together.

1. Introduction

This essay will review ethical aspects of computer and information security and privacy. Computer security is discussed in sections 2 and 3, and privacy in sections 4 and 5. A concluding section ties the two topics together.

Ethics is a field of study that is concerned with distinguishing right from wrong, and good from bad. It analyzes the morality of human behaviors, policies, laws and social structures. Ethicists attempt to justify their moral judgments by reference to ethical principles of theories that attempt to capture our moral intuitions about what is right and wrong. The two theoretical approaches that are most common in ethics are *consequentialism* and *deontology*. Consequentialist approaches assume that actions are wrong to the extent that they have bad consequences, whereas deontological approaches assume that people have moral duties that exist independently of any good or bad consequences that their actions may have. Ethical principles often inform legislation, but it it recognized in ethics that legislation cannot function as a substitute for morality. It is for this reason that individuals and corporations are always required to consider not only the legality but also the morality of their actions.

Ethical analysis of security and privacy issues in information technology primarily takes place in *computer ethics* which emerged in the 1980s as a field [1, 2]. Computer ethics analyzes moral responsibilities of computer professionals and computer users and ethical issues in public policy for information technology development and use. It asks such questions as: Is it wrong for corporations to read their employee's e-mail? Is it morally permissible for computer users to copy copyrighted software? Should people be free to put controversial or pornographic content online without censorship? Ethical issues and questions like these require *moral* or *ethical analysis*: analysis in which the moral dilemmas contained in these issues are clarified and solutions are proposed for them. Moral analysis aims to get clear on the facts and values in such cases, and to find a balance between the various values, rights and interests that are at stake and to propose or evaluate policies and courses of action.

2. Computer Security and Ethics

We will now turn to ethical issues in computer and information security. In this section, the moral importance of computer security will be assessed, as well as the relation between computer security and national security. Section 3 will consider specific ethical issues in computer security.

2.1 The Moral Importance of Computer Security

Computer security is a field of computer science concerned with the application of security features to computer systems to provide protection against the unauthorized disclosure, manipulation, or deletion of information, and against denial of service. The condition resulting from these efforts is also called computer security. The aim of computer security professionals is to attain protection of valuable information and system resources. A distinction can be made between the security of system resources and the security of information or data. The first may be called *system security*, and the second *information security* or *data security* [3]. System security is the protection of the hardware and software of a computer system against malicious programs that sabotage system resources. Information security is the protection of data that resides on disk drives on computer systems or is transmitted between systems. Information security is customarily defined as concerned with the protection of three aspects of data: their *confidentiality*, *integrity* and *availability*.

How does computer security pose ethical issues? As explained earlier, ethics is mostly concerned with rights, harms and interests. We may therefore answer this question by exploring the relation between computer security and rights, harms and interests. What morally important benefits can computer security bring? What morally important harms or violations of moral rights can result from a lack of computer security? Can computer security also cause harms or violate rights instead of preventing and protecting them?

A first and perhaps most obvious harm that can occur from breaches of computer security is economic harm. When system security is undermined, valuable hardware and software may be damaged or corrupted and service may become unavailable, resulting in losses of time, money and resources. Breaches of information security may come at an even higher economic cost. Valuable data may be lost or corrupted that is worth much more than the hardware on which it is stored, and this may cause severe economic losses. Stored data may also have personal, cultural or social value, as opposed to economic value, that can be lost when data is corrupted or lost. Any type of loss of system or data security is moreover likely to cause some amount of psychological or emotional harm.

Breaches of computer security may even cause grave harms like injury and death. This may occur in so-called *safety-critical systems*, which are computer systems with a component or real-time control that can have a direct life-threatening impact. Examples are computer systems in nuclear-reactor control, aircraft and air traffic control, missile systems and medical-treatment systems. The corruption of certain other types of systems may also have life-threatening consequences in a more indirect way. These may include systems that are used for design, monitoring, diagnosis or decision-making, for instance systems used for bridge design or medical diagnosis.

Compromises of the *confidentiality* of information may cause additional harms and rights violations. Third parties may compromise the confidentiality of information by accessing, copying and disseminating it. Such actions may, first of all, violate *property rights*, including *intellectual property rights*, which are rights to own and use intellectual creations such as artistic or literary works and industrial designs [4]. The information may be exclusively owned by someone who has the right to determine who can access and use the information, and this right can be violated.

Second, compromises of confidentiality may violate *privacy rights*. This occurs when information that is accessed includes information about persons that is considered to be private. In addition to violations of property and privacy rights, breaches of confidentiality may also cause a variety of other harms resulting from the dissemination and use of confidential information. For instance, dissemination of internal memos of a firm damages its reputation, and compromises of the confidentiality of online credit card transactions undermines trust in the security of online financial transactions and harms e-banking and e-commerce activity.

Compromises of the *availability* of information can, when they are prolonged or intentional, violate *freedom rights*, specifically rights to freedom of information and free speech. *Freedom of information* is the right to access and use public information. Jeroen van den Hoven has argued that access to information has become a moral right of citizens in the information age, because information has become a primary social good: a major resource necessary for people to be successful in society [5]. Shutting down vital information services could violate this right to information. In addition, computer networks have become important as a medium for speech. Websites, e-mail, bulletin boards, and other services are widely used to spread messages and communicate with others. When access to such services is blocked, for instance through denial of service attacks or hijackings of websites, such acts are properly classified as violations of *free speech*.

Computer security measures normally prevent harms and protect rights, but they can also cause harm and violate rights. Notably, security measures may be so protective of information and system resources that they discourage or prevent stakeholders from accessing information or using services. Security measures may also be discriminatory: they may wrongly exclude certain classes of users from using a system, or may wrongly privilege certain classes of users over others.

2.2 Computer Security and National Security

Developments in computer security have been greatly influenced by the September 11, 2001 terrorist attacks in the United States and their aftermath. In response to these attacks, national security has become a major policy concern of Western nations. *National security* is the maintenance of the integrity and survival of the nation-state and its institutions by taking measures to defend it from threats, particularly threats from the outside. Many new laws, directives and programs protective of national security have come into place in Western nations after 9/11, including the creation in the U.S. of an entire Department of Homeland Security. The major emphasis in these initiatives is the protection of state interests against terrorist attacks [6].

Information technology has acquired a dual role in this quest for national security. First of all, computer security has become a major priority, particularly the protection of critical information infrastructure from external threats. Government computers, but also other public and private infrastructure, including the Internet and telephone network, have been subjected to stepped-up security measures. Secondly, governments have attempted to gain more control over public and private information infrastructures. They have done this through wiretapping and data interception, by requiring Internet providers and telephone companies to store phone and e-mail communications records and make them available to law enforcement officials, by attempting to outlaw certain forms of encryption, or even through attempts to require companies to reengineer Internet so that eavesdropping by the government is made easier. Paradoxically, these efforts by governments to gain more control over information also lessen certain forms of security: they make computers less secure from access by government agencies.

Philosopher Helen Nissenbaum has argued that the current concern for national security has resulted in a new conception of computer security next to the classical one [7]. The classical or ordinary conception of computer security is the one used by the technical community and defines computer security in terms of systems security and integrity, availability and confidentiality of data (see section 2.1). Nissenbaum calls this *technical computer security*. The other, which she calls *cybersecurity*, involves the protection of information infrastructure against threats to national interests. Such threats have come to be defined more broadly than terrorism, and have nowadays come to include all kinds of threats to public order, including internet crime, online child pornography, computer viruses, and racist and hate-inducing websites. At the heart of cybersecurity, however, are concerns for national security, and especially the state's vulnerability to terrorist attacks.

Nissenbaum emphasizes that technical computer security and cybersecurity have different conceptions of the aims of computer security and the measures that need to be taken. Technical computer security aims to protect the private interests of individuals and organizations, specifically owners and users of computer systems and data. Cybersecurity aims to protect the interests of the nation-state and conceives of computer security as a component of national security. Technical computer security measures mostly protect computer systems from outside attacks. Cybersecurity initiatives include such protective measures as well, but in addition include measures to gain access to computer systems and control information. The two conceptions of security come into conflict when they recommend opposite measures. For instance, cyber-security may require computers system to be opened up to remote government inspection or may require government access to websites to shut them down, while technical computer security may prohibit such actions. The different interests of technical computer security and cybersecurity can in this way create moral dilemmas: should priority be given to state interests or to the interests and rights of private parties? This points to the larger dilemma of how to balance national security interests against civil rights after 9/11 [8].

3. Ethical Issues in Computer Security

In this section, ethical aspects of specific practices in relation to computer security will be analyzed. Section 3.1 and 3.2 will focus on practices that undermine computer security: hacking, computer crime, cyberterrorism and information warfare. Section 3.3 will consider the moral responsibilities of information security professionals.

3.1 Hacking and Computer Crime

A large part of computer security is concerned with the protection of computer resources and data against unauthorized, intentional break-ins or disruptions. Such actions are often called *hacking.* Hacking, as defined in this essay, is the use of computer skills to gain unauthorized access to computer resources. Hackers are highly skilled computer users that use their talents to gain such access, and often form communities or networks with other hackers to share knowledge and data. Hacking is often also defined, more negatively, as the gaining of such unauthorized access for malicious purposes: to steal information and software or to corrupt data or disrupt system operations. Self-identified hackers, however, make a distinction between non-malicious break-ins, which they describe as hacking, and malicious and disruptive break-ins, which they call *cracking* [9].

Self-identified hackers often justify their hacking activities by arguing that they cause no real harm and instead have a positive impact. The positive impact of hacking, they argue, is that it frees data to the benefit of all, and improves systems and software by exposing security holes. These considerations are part of what has been called the *hacker ethic* or *hacker code of ethics* [10, 11], which is a set of (usually implicit) principles that guide the activity of many hackers. Such principles include convictions that information should be free, that access to computers should be unlimited and total, and that activities in cyberspace cannot do harm in the real world.

Tavani has argued that many principles of the hacker ethic cannot be sustained [1]. The belief that information should be free runs counter to the very notion of intellectual property, and would imply that creators of information would have no right to keep it to themselves and have no opportunity to make a profit from it. It would moreover fundamentally undermine privacy, and would undermine the integrity and accuracy of information, as information could be modified and changed at will by anyone who would access it. Tavani also argues that the helpfulness of hacking in pointing to security weaknesses may not outweigh the harm it does, and that activities in cyberspace can do harm in the real world.

Both hacking and cracking tend to be unlawful, and may therefore be classified as a form of computer crime, or cybercrime, as it has also been called [12]. There are many varieties of computer crime, and not all of them compromise computer security. There are two major types of cybercrime that compromise computer security: *cybertrespass*, which is defined by Tavani ([1], p. 193) as the use of information technology to gain unauthorized access to computer systems or password-protected websites, and *cybervandalism*, which is the use of information technology to unleash programs that disrupt the operations of computer networks or corrupt data.

Tavani distinguishes a third type of cybercrime that sometimes includes breaches of computer security, *cyberpiracy*. Cyberpiracy, also called *software piracy*, is the use of information technology to reproduce copies of proprietary software or information or to distribute such data across a computer network. Cyberpiracy is much more widespread than cybervandalism or cybertrespass, because it does not require extensive computer skills and many computer users find it morally permissible to make copies of copyrighted software and data. Cyberpiracy involves breaches in computer security when it includes the cracking of copyright protections.

Another type of cybercrime that sometimes involves breaches of computer security is *computer fraud*, which is deception for personal gain in online business transactions by assuming a false online identity or by altering or misrepresenting data.[1] Computer fraud may depend on acts of cybertrespass to obtain passwords, digital identities, or other transaction or access codes, and acts of cybervandalism involving the modification of data. Other types of cybercrime, such as the online distribution of child pornography or online harassment and libel, usually do not involve breaches of computer security.

[1] When the identity used in computer fraud is “borrowed” from someone else, this is called *identity theft*.

3.2 Cyberterrorism and Information Warfare

A recent concern in computer and national security has been the possibility of *cyberterrorism*, which is defined by Herman Tavani as the execution of "politically motivated hacking operations intended to cause grave harm, that is, resulting in either loss of life or severe economic loss, or both" ([1], p. 161). The possibility of major attacks on information infrastructure, intending to debilitate or compromise this infrastructure and harm economic, industrial or social structures dependent on it, has become a major concern since the 9/11 attacks. Such attacks could be both foreign and domestic.

Controversy exists on the proper scope of "cyberterrorism". Where should the boundaries be drawn between cyberterrorism, cybercrime, and cybervandalism? Should a teenager who releases a dangerous virus that turns out to cause major harm to government computers be persecuted as a cyberterrorist? Are politically motivated hijackings of the homepages of major organizations acts of cyberterrorism? A distinction between cyberterrorism and other kinds of cyberattacks may be found in its political nature: cyberterrorism consists of politically motivated operations that aim to cause harm. Yet, Mark Mainon and Abby Goodrum [13] have argued that not all politically motivated cyberattacks should be called cyberterrorism. They distinguish cyberterrorism from *hacktivism*, which are hacking operations against an internet site or server with the intent to disrupt normal operations but without the intent to cause serious damage. Hacktivists may make use of e-mail bombs, low-grade viruses, and temporary homepage hijackings. They are politically motivated hackers who engage in a form of electronic political activism that should be distinguished from terrorism [14].

Information warfare is an extension of ordinary warfare in which combatants use information and attacks on information and information systems as tools of warfare [15, 16]. Information warfare may include the use of information media to spread propaganda, the disruption, jamming or hijacking of communication infrastructure or propaganda feeds of the enemy, and hacking into computer systems that control vital infrastructure (e.g., oil and gas pipelines, electric power grids, or railway infrastructure).

3.3 Moral Responsibilities of Information Security Professionals

Information security (IS) professionals are individuals whose job it is to maintain system and information security. By standing of their profession, they have a professional responsibility to assure the correctness, reliability, availability, safety and security of all aspects of information and information systems. The discussion in section 2 makes clear that this responsibility has a moral dimension: professional activities in computer security may protect people from morally important harms but could also cause such harms, and may either protect or violate people's moral rights. In case of safety-critical systems, the decisions of information security professionals may even be a matter of life or death.

That IS professionals have moral responsibilities as part of their profession is reflected in codes of ethics used by various organizations for computer and information security. These codes of ethics rarely go into detail, however, on the moral responsibilities of IS professionals in specific situations. For instance, the code of ethics of the Information Systems Security Association (ISSA), an international organization of information security professionals and practitioners, only states that members should "[p]erform all professional activities and duties in accordance with all applicable laws and the highest ethical principles" but does not go on to specify what these ethical principles are or how they should be applied and balanced against each other in specific situations [17].

For IS professionals, as well as for other computer professionals who have a responsibility for computer security, a code of ethics clearly is not enough. To appreciate the moral dimension of their work, and to cope with moral dilemmas in it, they require training in information security ethics. Such training helps professionals to get clear about interests, rights, and moral values that are at stake in computer security, to recognize ethical questions and dilemmas in their work, and to balance different moral principles in resolving such ethical issues [18].

4. Information Privacy and Ethics

We will now turn to issues of privacy in modern data management. In this section, it will be considered what privacy is, why it is important and how it is impacted by information technology. Section 5 will then consider major privacy issues in modern data management.

4.1 What is Privacy and Why is It Important?

In Western societies, a broad recognition exists of a right to personal privacy. The right to privacy was first defended by the American justices Samuel Warren and Louis Brandeis, who defined privacy as "the right to be let alone" [19]. Privacy is a notion that is difficult to define, and many more precise definitions have since been presented. Often, the right to privacy is defined as the right of individuals to control access or interference by others into their private affairs. Philosopher Ferdinand Schoeman has defined it thus: "A person has privacy to the extent that others have limited access to information about him, limited access to the intimacies of his life, or limited access to his thoughts or his body." ([20], p. 3). Schoeman's definition shows that the concept of privacy does not only apply to the processing of personal information. It also applies to the observation of and interference with human behaviors and relations, the human body, and one's home and personal belongings [21].

Privacy is held to be valuable for several reasons. Most often, it is held to be important because it is believed to protect individuals from all kinds of external threats, such as defamation, ridicule, harassment, manipulation, blackmail, theft, subordination, and exclusion. James Moor has summed this up by claiming that privacy is an articulation of the core value of *security*, meant to protect people from all kinds of harm done by others [22]. It has also been argued that privacy is a necessary condition for *autonomy*: without privacy, people could not experiment in life and develop their own personality and own thoughts, because they would constantly be subjected to the judgment of others. The right to privacy has also been claimed to protect other rights, such as abortion rights and the right to sexual expression. Privacy moreover has been claimed to have social value in addition to individual value. It has, for instance, been held to be essential for maintaining democracy [23].

The right to privacy is not normally held to be absolute: it must be balanced against other rights and interests, such as the maintenance of public order and national security. Privacy rights may also vary in different contexts. There is, for example, a lesser expectation of privacy in the workplace or in the public sphere than there is at home. An important principle used in privacy protection in Western nations is that of *informed consent*: it is often held that citizens should be informed about how organizations plan to store, use or exchange their personal data, and that they should be asked for their consent. People can then voluntarily give up their privacy if they choose.

4.2 Information Technology and Privacy

Privacy is a value in modern societies that corresponds with the ideal of the autonomous individual who is free to act and decide his own destiny. Yet, modern societies are also characterized by surveillance, a practice that tends to undermine privacy. *Surveillance* is the systematic observation of (groups of) people for specific purposes, usually with the aim of exerting some form of influence over them. Sociologist David Lyon has argued that surveillance has always been an important part of modern societies [24]. The state engages in surveillance to protect national security and to fight crime, and the modern corporation engages in surveillance in the workplace to retain control over the workforce.

Computerization from the 1960s onward has intensified surveillance by increasing its scale, ease and speed. Surveillance is partially delegated to computers that help in collecting, processing and exchanging data. Computers have not only changed the scale and speed of surveillance, they have also made a new kind of surveillance possible: *dataveillance*, which is the large-scale, computerized collection and processing of personal data in order to monitor people's actions and communications [25]. More and more, information technology is not just used to record and process static information about individuals, but to record and process their actions and communications. New detection technologies like smart closed-circuit television (CCTV), biometrics and Intelligent User Interfaces, and new data processing techniques like data mining further exacerbate this trend. As Lyon has argued, the ease with which surveillance now takes place has made it a generalized activity that is routinely performed in all kinds of settings by different kinds of organizations. Corporations, for instance, have extended surveillance from the workplace to their customers (*consumer surveillance*). In addition, the 9/11 terrorist attacks have drastically expanded surveillance activities by the state.

Many privacy disputes in today's society result from tensions between people's right to privacy and state and corporate interests in surveillance. In the information society, privacy protection is realized through all kinds of information privacy laws, policies and directives, or *data protection* policies, as they are often called in Europe. These policies regulate the harvesting, processing, usage, storage and exchange of personal data. They are often overtaken, however, by new developments in technology. However, privacy protection has also become a concern in the design and development of information technology.

Information privacy has also become a major topic of academic study. Studies of information privacy attempt to balance privacy rights against other rights and interests, and try to determine privacy rights in specific contexts and for specific practices. Specialized topics include workplace privacy [26], medical privacy [27], genetic privacy [28], Internet privacy (section 5.1), and privacy in public (section 5.3).

5. Privacy Issues in Modern Data Management

5.1 Internet Privacy

The Internet raises two kinds of privacy issues. First, the posting and aggregation of personal information on Internet websites sometimes violates privacy. Websites on the Internet contain all sorts of personal information that is made publicly available, often without the bearer's explicit consent. They may contain, for instance, one's phone number and address, archived bulletin board messages from years past, information about one's membership of organizations, online magazines and newspapers in which one is mentioned, online databases with public records, pictures and video clips featuring oneself, etc. Using search engines, this information can easily be located and be used to create elaborate composite records about persons (see section 5.2). Should there be limits to this? When should someone's consent be asked when his personal information is posted on the web, or when such information is used for specific purposes? (See also section 5.3).

A second type of privacy issue involves the online monitoring of internet users. Their connection to the internet may be used by third parties to collect information about them, in a way that is often invisible to them. Online privacy risks include *cookies* (small data packets placed by servers on one's computer for user authentication, user tracking, and maintaining user-specific information), *profiling* or *tracking* (recording the browsing behavior of users), and *spyware* (computer programs that maliciously collect information from a user's computer system or about a user's browser behavior and send this information over the internet to a third party). In addition, private e-mail and data traffic may be intercepted at various points, for instance by employers, internet service providers, and government agencies. When do such actions violate privacy, and what should be done to protect internet privacy? [29].

5.2 Record Merging and Matching and Data Mining

It frequently happens that different databases with personal information are combined to produce new data structures. Such combinations may be made in two ways ([1], p. 127-131). First, the records in two databases may be *merged* to produce new composite records. For instance, a credit card company may request information about its prospective customers from various databases (e.g., financial, medical, insurance), which are then combined into one large record. This combined record is clearly much more privacy-sensitive than the records that compose it, as the combined record may generate perceptions and suggest actions that would not have resulted from any of the individual records that make it up.

Second, records in databases may be *matched*. Computer matching is the cross-checking in two or more unrelated databases for information that fits a certain profile in order to produce matching records or "hits". Computer matching is used often by government agencies to detect possible instances of fraud or other crimes. For instance, ownership records of homes or motorized vehicles may be matched with records of welfare recipients to detect possible instances of welfare fraud. Computer matching has raised privacy concerns because it is normally done without the consent of the bearers of personal information that are involved. Moreover, matches rarely prove facts about persons but rather generate suspicions that require further investigation. In this way, record matching could promote stereotyping and lead to intrusive investigations.

Data Mining is a technique that is usually defined over a single database. It is the process of automatically searching large volumes of data for patterns, using techniques like statistical analysis, machine learning and pattern recognition. When data mining takes place in databases containing personal information, the new information thus gained may be privacy-sensitive or confidential even when the old information is not. It may for instance uncover patterns of behavior of persons that were not previously visible. Data mining may also be used to stereotype whole categories of individuals. For instance, a credit card company may use data mining on its customer database to discover that certain zip codes correlate strongly with loan defaults. It may then decide not to extend credit anymore to customers with these zip codes. In summary, data mining may violate individual privacy and may be used to stereotype whole categories of individuals. Ethical policies are needed to prevent this from happening [30].

5.3 Privacy in Public

It is sometimes believed that privacy is a right that people have when they are in private places like homes, private clubs and restrooms, but that is minimized or forfeited as soon as they enter public space. When you walk in public streets or are on the road with your car, it is sometimes believed, you may retain the right not to be seized and searched without probable cause, but your appearance and behavior may be freely observed, surveilled and registered. Many privacy scholars, however, have argued that this position is not wholly tenable, and that people have privacy rights in public areas that are incompatible with certain registration and surveillance practices [31, 32].

The problem of privacy in public applies to the tracking, recording, and surveillance of public appearances, movements and behaviors by individuals and their vehicles. Techniques that are used for this including video surveillance (CCTV), including smart CCTV for facial recognition, infrared cameras, satellite surveillance, GPS tracking, RFID tagging, electronic checkpoints, mobile phone tracking, audio bugging, and ambient intelligence techniques. Does the use of these techniques violate privacy even when they are used in public places? The problem of privacy in public also applies to publicly available information on the Internet, as discussed in section 5.1. Does the fact that personal information is available on a public forum make it all right to harvest this information, aggregate it and use it for specific purposes?

Helen Nissenbaum has argued in an influential paper that surveillance in public places that involves the electronic collection, storage and analysis of information on a large scale often amounts to a violation of personal privacy [31]. She argues that people often experience such surveillance as an invasion of their privacy if they are properly informed about it, and that such electronic harvesting of information is very different from ordinary observation, because it shifts information from one context to another and frequently involves record merging and matching and data mining. She concludes that surveillance in public places violates privacy whenever it violates *contextual integrity*: the trust that people have that acquired information appropriate to one context will not be used in other contexts for which it was not intended.

5.4 Biometric Identification

Biometrics is the identification or verification of someone's identity on the basis of physiological or behavioral characteristics. Biometric technologies provide a reliable method of access control and personal identification for governments and organizations. However, biometrics has also raised privacy concerns [33]. Widespread use of biometrics would have the undesirable effect of eliminating anonymity and pseudonymity in most daily transactions, because people would leave unique traces everywhere they go. Moreover, the biometric monitoring of movements and actions gives the monitoring organization insight into a person’s behaviors which may be used against that person’s interests. In addition, many people find biometrics distasteful, because it involves the recording of unique and intimate aspects *of* (rather than *about*) a person, and because biometric identification procedures are sometimes invasive of bodily privacy. The challenge for biometrics is therefore to develop techniques and policies that are optimally protective of personal privacy.

5.5 Ubiquitous Computing and Ambient Intelligence

Ubiquitous Computing is an approach in information technology that aims to move computers away from the single workstation and embed microprocessors into everyday working and living environments in an invisible and unobtrusive way. *Ambient Intelligence* is an advanced form of ubiquitous computing that incorporates wireless communication and Intelligent User Interfaces, which are interfaces that use sensors and intelligent algorithms for profiling (recording and adapting to user behavior patterns) and context awareness (adapting to different situations) [34]. In Ambient Intelligence environments, people are surrounded with possibly hundreds of intelligent, networked computers that are aware of their presence, personality and needs, and perform actions or provide information based on their perceived needs.

Marc Langheinrich [35] has claimed that ubiquitous computing has four unique properties that are potentially threatening to privacy: (1) *ubiquity*; (2) *invisibility*; (3) *sensing*; (4) *memory amplification* (the continuous recording of people's actions to create searchable logs of their past). I have argued that Ambient Intelligence adds two properties to this list: (5) *user profiling*; and (6) *connectedness* (wireless communication between smart objects) [36].

These unique features of the two technologies make the protection of privacy in them a major challenge. As critics have argued, ubiquitous computing and ambient intelligence have the ability to create a Big Brother society in which every human activity is recorded and smart devices probe people's actions, intentions and thoughts. The distinction between the private and the public sphere may be obliterated as dozens of smart devices record activity in ones home or car and connect to corporate or government computers elsewhere. Major privacy safeguards will be needed to avoid such scenarios (see chapter 28 in this volume for a discussion of privacy protection in Ambient Intelligence).

6. Conclusion

Privacy is a moral right of individuals that is frequently and increasingly at issue when information systems are used. It was explained in this essay why privacy is important and how it is impacted by information technology, and various ethical issues in information privacy were reviewed. Computer security is not itself a moral right or moral value, but it has been argued that maintaining computer security may be morally necessary to protect correlated rights and interests: privacy rights, property rights, freedom rights, human life and health and national security. It was argued that computer security can also work to undermine rights.

Ethical analysis of privacy and security issues in computing can help computer professionals and users recognize and resolve moral dilemmas and can yield ethical policies and guidelines for the use of information technology. In addition, it has been recognized in computer ethics that not only the use of information systems requires moral reflection, but also their design, as system designs reflect moral values and involve moral choices [37, 38]. A system can for example be designed to protect privacy, but it can also be designed to give free access to personal information to third parties. This fact is taken up in *value-sensitive design*, an approach to the design of information systems that attempts to account for values in a principled fashion [39]. Ideally, ethical reflection on information technology should not wait until products hit the market, but should be built in from the beginning by making it part of the design process.

References

1. Tavani, H.:. *Ethics and Technology: Ethical Issues in an Age of information and Communication Technology* (Wiley, 2004)
2. Johnson, D.: *Computer Ethics*, 3rd edn (Upper Sadle River: Prentice Hall, 2000)
3. Spinello, R. and Tavani, H.: Security and Cyberspace. In: *Readings in Cyberethics*, 1st edn, ed by Spinello R., and Tavani, H. (Jones and Bartlett, Sudbury MA, 2001) pp. 443-450
4. Halbert, D.: *Intellectual Property in the Information Age: The Politics of Expanding Ownership Rights*. (Quorum Books, Westport CT, 1999)
5. Hoven, J. van den (1995). Equal Access and Social Justice: Information as A Primary Good. In: *Proceedings of ETHICOMP95, vol. 1* (DeMontfort University, Leicester UK, 1995)

6. Bullock, J., et al.: *Introduction to Homeland Security,* 1st edn *(*Butterworth-Heinemann, 2005)
7. Nissenbaum, H.: Where Computer Security Meets National Security. *Ethics and Information Technology* **7**, 61-73 (2005).
8. Davis, D. and Silver, B.: Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science* **48**(1), 28-46 (2004)
9. Himma, K. (ed.): *Readings on Internet Security: Hacking, Counterhacking, and Other Moral Issues* (Jones & Bartlett, forthcoming)
10. Levy, S.: *Hackers: Heroes of the Computer Revolution*. (Doubleday, Garden City NY, 1984)
11. Himanen, P.: *The Hacker Ethic: A Radical Approach to the Philosophy of Business (*Random House, New York, 2001).
12. McQuade, S,: *Understanding and Managing Cybercrime* (Allyn & Bacon, 2005).
13. Mainon, D. and Goodrum, A.: Terrorism or Civil Disobedience: Toward a Hacktivist Ethic. *Computers and Society*, **30**(2), 14-19 (2000)
14. Denning, D.: Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy. In: *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed Arquilla, J., Ronfeldt, D. (Rand Corporation, 2002). Also online at http://www.rand.org/publications/MR/MR1382/.
15. Denning, D.: *Information Warfare and Security* (Addison-Wesley, Reading MA, 1999)
16. Rattray, G.: *Strategic Warfare in Cyberspace* (MIT Press, Cambridge MA, 2001)
17. ISSA: ISSA Code of Ethics. In: Information Systems Security Association Website. http://www.issa.org/codeofethics.html (2005). Cited 14 Mar 2006
18. Bynum, T. and Rogerson, S. (eds.): *Computer Ethics and Professional Responsibility: Introductory Text and Readings* (Blackwell, 2003)
19. Warren, S. and Brandeis, L.: The Right to Privacy. *Harvard Law Review* **4**, 193-220 (1890)
20. Schoeman, F.: Introduction. In: *Philosophical Dimensions of Privacy: An Anthology*, ed. Schoeman, F. (Cambridge University Press, Cambridge UK, 1984)
21. Brey, P.: The Importance of Privacy in the Workplace. In: *The Ethics of Privacy in the Workplace,* ed S. O. Hansson, S., Palm, E. (Peter Lang, Brussels, 2005) pp. 97-118
22. Moor, J.: Towards a Theory of Privacy for the Information Age. *Computers and Society* **27**(3), 27-32 (1997)
23. Westin, A.: *Privacy and Freedom* (Atheneum, New York, 1967)
24. Lyon, D.: *Surveillance Society. Monitoring Everyday Life (*Open University Press, Buckingham UK, 2001)
25. Clarke, R.: Information Technology and Dataveillance. *Communications of the ACM* **31**(5), 498-512 (1988)
26. Hansson, S. and Palm, E. (eds.): *The Ethics of Privacy in the Workplace (*Peter Lang, Brussels, 2005)

27. Steward, M. Electronic Medical Records – Privacy, Confidentiality, Liability. *Journal of Legal Medicine* **26**(4), 491-506 (2005)
28. Laurie, Graeme T.: *Genetic Privacy: A Challenge to Medico-Legal Norms* (Cambridge University Press, Cambridge UK, 2002)
29. Bennett, C.: Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web. *Ethics and Information Technology* **3**(3), 195 – 208 (2001)
30. Van Wel, L. and Royakker, L.: Ethical Issues in Web Data Mining. *Ethics and Information Technology* **6**, 129–140 (2004)
31. Nissenbaum, H.: Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy* **17**: 559-596 (1998)
32. Brey, P.: Ethical Aspects of Face Recognition Systems in Public Places. In: *Readings in Cyberethics*, 2nd edn, ed by Spinello, R., Tavani, H. (Jones and Bartlett, Sudbury, MA, 2004) pp. 585-600
33. Clarke, R.: Biometrics and Privacy. http://www.anu.edu.au/people/Roger.Clarke/ DV/Biometrics.html (2001). Cited 15 Mar 2006
34. Weber, W., Rabaey, J. and Aarts, E. (eds.): *Ambient Intelligence* (Springer, Berlin Heidelberg New York, 2005)
35. Langheinrich, M.: Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. In: *Lecture Notes In Computer Science; Vol. 2201 Archive.* (Springer, Berlin Heidelberg New York, 2001), pp. 273 - 291
36. Brey, P.: Freedom and Privacy in Ambient Intelligence. *Ethics and Information Technology* **7**, 157-166 (2006)
37. Nissenbaum, H.: Values in Technical Design. In: *Encyclopedia of Science, Technology and Society*, ed. by Mitcham, C. (MacMillan, New York, 2005), lxvi-lxx
38. Brey, P.: Disclosive Computer Ethics. *Computers and Society* **30**(4), 10-16 (2000)
39. Friedman, B.: Value Sensitive Design. *Encyclopedia of Human-Computer Interaction* (Great Barrington, MA: Berkshire, 2004) pp. 769-774