Chapter X

Responsibility for Information Assurance and Privacy: A Problem of Individual Ethics?

Bernd Carsten Stahl, De Montfort University, UK

ABSTRACT

Decisions regarding information assurance and IT security can affect individuals’ rights and obligations and thereby acquire a moral quality. The same can be said for questions of privacy. This chapter starts by showing how and why information assurance and privacy can become problems worthy of ethical consideration. It demonstrates that there is no simple and linear relationship between ethics and information assurance or between ethics and privacy. Many decisions in the area of IT, however, affect not only one, but both of these subjects. The ethical evaluation of decisions and actions in the area of privacy and security, therefore, is highly complex. This chapter explores the question whether individual responsibility is a useful construct to address ethical issues of this complexity. After introducing a theory of responsibility, this chapter discusses the conditions that a subject of responsibility typically is assumed to fulfill. This chapter will argue that individual human beings lack some of the
essential preconditions necessary to be ascribed responsibility. Individuals have neither the power, the knowledge, nor the intellectual capacities to deal successfully with the ethical challenges in the tension of privacy and information assurance. This chapter ends by suggesting that the concept of responsibility, nevertheless, may be useful in this setting, but it would have to be expanded to allow collective entities as subjects.

INTRODUCTION

Proponents of information assurance aim at meeting the security testing, evaluation, and assessment needs of IT consumers and producers. They are mostly interested in eliminating security threats and, in the long run, want to increase the levels of trust that users and consumers have in IT and networks. While most users support these goals of information assurance, they also have other objectives when using IT; among them is the preservation of privacy. To a certain degree, these two objectives are contradictory. In order to facilitate security, it would be helpful to eliminate privacy, because this would allow an easier detection and elimination of security risks. Privacy, on the other hand, requires security, because the protection of private data relies on the assumption that no unauthorized access is possible. Privacy and information assurance thus also can be complementary.

Further complicating this relationship, both terms also have an ethical side to them. Trust, as the ultimate aim of information assurance, is at least partly a moral notion. Security is necessary to facilitate a free and equal exchange of ideas. At the same time, an excess of security can stifle the exchange of ideas and the greater good. Privacy generally is recognized as a moral good, but it is debatable how this good can be justified and where its limits are. The individual user, who must make decisions concerning the weighting of privacy and information assurance, therefore finds himself in a situation where, despite an ethical quality of the choices, it is less than clear how decisions are to be made.

This is where the concept of responsibility enters the picture. This chapter will describe a theory of responsibility and put a special emphasis on the question of who can be the subject of responsibility. This theory of responsibility then will be applied to the complex problem of privacy and information assurance. The theory and conditions of responsibility will be used to demonstrate that while individual responsibility can play an important role in such ethical decisions, it also runs into severe problems. It will be argued that due to the lack of fulfillment of the basic conditions of responsibility, the individual end user is not able to shoulder the burdens required in order to make an ethical decision. As a consequence, questions of privacy and information assurance require a wider context and frame in which they can be answered. Only in such a frame does individual responsibility make sense and can it achieve its objectives.
How should the individual end user deal with this dilemma? The conclusion of the chapter will argue that the content of this chapter is of high relevance for the individual end user, because it allows him or her to recognize the limits of his or her capacities. The very fact that individual humans quickly reach their fundamental limits when they are ascribed responsibility in the context of information assurance and privacy will allow them to overcome their limitations. By pointing out why they cannot accept such responsibility ascriptions, they should be able to transcend the ascription and open discourses that will include other subjects, which, in turn, might be able to solve the problem. Briefly, the arguments presented in this chapter can be used to protect the individual end user from responsibility ascription that he or she is incapable of satisfying. At the same time, they should help avoid situations where responsibility is wrongly ascribed to individuals.

INFORMATION ASSURANCE AND PRIVACY: AN ETHICAL CHALLENGE

As indicated in the introduction, a brief look at the concepts of information assurance and privacy could suggest that the two can be contradictory, but the opposite interpretation is just as possible. Since it is the purpose of this chapter to analyze the role that individual responsibility can play with regard to the realization of information assurance and privacy, this section will be dedicated to a discussion and definition of the concepts. In both cases, the focus of the discussion will be their ethical content and the ethical challenges they pose.

We will leave the definition of ethics as open as possible and work with a common sense notion of ethics. While this may not be very satisfactory from a philosophical point of view, one reason to support this approach is that most end users who make moral decisions concerning the use of ICT do not have a formal education in philosophical ethics. At the same time, most users probably can be considered to be ethical in the sense that they want to do the right thing. In order to do so, they need some sort of private understanding of ethics, and it is this that we will work with here. Briefly, ethics here will be understood as having to do with doing good. Ethical behavior aims at improving the circumstances of oneself and, more importantly, of others. Part of this is to respect other people’s rights and interests, and in order to determine these, one has to assume a basic similarity of rights and interests between different people. A generally shared rule of pre-theoretical ethics, which is also reflected in ethical theories, is to treat the other in such a way as one wants to be treated oneself. This rough sketch of ethics will suffice for the identification of ethical problems posed by information assurance and privacy. The reader who is not satisfied with this concept of ethics is referred to Stahl (2004) for a detailed discussion of the relationship of philosophical ethics and the idea of reflective responsibility.
The Ethics of Information Assurance

Information assurance is a term that denotes the idea of security of information in technical systems. The U.S. National Information Assurance Partnership, for example, is a government initiative “designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers” (NIAP 2003, p. ). Information assurance tends to focus on security in information systems using a relatively wide framework. As the above definition shows, it is a collaborative effort of private, public, and often academic institutions that endeavors to consider all of the relevant stakeholders. While not a completely new idea, the information assurance movement seems to have been strengthened by the September 11, 2000, terrorist attack and the subsequent attention by governments, particularly the U.S. federal government, to security threats. This is shown by the fact that the U.S. military plays a prominent role in information assurance (IASE 2003). This close connection of information assurance to terrorism, government, and the military carries ethical implications by itself that this chapter will not be able to discuss. For the purposes of this chapter, we will understand information assurance as concerned with the security in information systems and, therefore, concentrate on the ethical implications of security.

Threats and Solutions to Security Problems

Threats to security and information assurance can be seen in many different areas. They can result from intentional attacks but also from unintended misbehavior or from technical or organizational mistakes. A central problem in rectifying these mistakes is that they not only are unknown but, by definition, unknowable. Human beings who make decisions regarding information technology deal with future states and, therefore, have to accept uncertainty and risks in their decisions (Grabner-Kräuter 2002).

Nevertheless, the knowledge of uncertainties and possible dangers compels us to act in order to avoid damages. In the case of threats to IT security, there are several areas where security efforts can be fruitful. Among them, one can find malicious attacks such as worms, viruses, and the like (Eisenberg et al., 1995) or hacking (Johnson 2001). The biggest fear at the moment is probably terrorism. It is interesting to note, however, that it is not a new fear and that connections between the use of IT and terrorist attacks have been predicted years before the attack on the World Trade Center (Levy 1995).

Information assurance, as the attempt to assure the availability of IT services, can go several routes and will usually take several of them simultaneously. On the one hand, there are organizational measures that are frequently linked with the embedding of information systems in organizations and hierarchies (Healy & Iles 2002). On the other hand, there are technical measures that include the setting of standards of reliability (Littlewood & Stringy 1995),
measures to ensure authentication such as biometrics (van der Ploeg 2001), or others such as encryption (Tavani 2000).

**The Ethical Implications of Information Assurance**

Given the loose definition of ethics used in this chapter, there are many possible points of contact where information assurance and security can have an ethical impact. If ethics has to do with doing the right thing (whatever that may mean in a particular situation), then security in IT is something of ethical relevance. Security questions affect who gets access to which technology. They determine who can communicate with whom and about which topics. Security regulations imply power relationships with all their ethical baggage. The question of reciprocity that was introduced as central to ethical thinking is affected by security measures. Generally, one can state that most, if not all, attempts to secure information technology affects in some way or other the way people can behave and interact. They thereby automatically affect moral rights and obligations. At the same time, security is also a necessary precondition for ethical action. In order to act ethically, one needs social norms and institutions that support and facilitate such action. This means that these institutions must be secured. On the other hand, security considerations can be misused as excuses for immoral behavior.

Information assurance thus can be seen as a topic of ethical importance that has no clear and unequivocal ethical message. Security measures can have morally positive results, but they can also become moral liabilities. There are no simple guidelines along the lines of the more security, the more ethics. Individuals making decisions regarding security are, therefore, in a difficult position when they want to consider ethical problems. This difficult situation is exacerbated when one widens possible decisions beyond pure security considerations and looks at other factors—in our case, privacy.

**The Ethics of Privacy**

Privacy is a concept that has gained prominence due to the spread of information technology and the approaching information society. Given the complexity of the discussion about privacy and the importance it has for the question of how to assume responsibility for it, this section first will look at the definitions of privacy, then at the justifications that can be found in the literature in order to analyze the limits of the concept.

**Definitions of Privacy**

There is much debate about privacy from different academic disciplines. One of the fields where privacy is most hotly debated is that of computer and information ethics. Most authors agree that privacy is a moral value. However, it often is not clear what exactly privacy is (Weckert & Adeney, 1997) and why
it must be considered valuable. However, the amount of protection we believe to be appropriate and the outcome of conflicts between privacy and other interests depend on our answer to these questions, which is why it is necessary in this chapter to give an overview of definition, justification, and limits of privacy.

Unlike information assurance, which is a term that only makes sense in a modern society and with the use of information technology in mind, privacy is an old concept that can be traced back to the beginning of modern civilization among the ancient Greeks (Rotenberg, 1998). The modern meaning and importance of the term privacy, nevertheless, are linked closely to technology. Also, the legal protection of privacy is a relatively new phenomenon dating back to the late 1800s, which coincides with the growth of cities and the migration from rural environments (Sipior & Ward, 1995). It is interesting to note that the legal protection of privacy was a reaction to a technological development; namely, photography. Warren and Brandeis (1890) wrote a seminal chapter that started the modern discussion about privacy and led to its legal codification because of the fact that through the use of technology, it became possible for the first time to make accurate pictures of someone without their consent. Warren and Brandeis (1890) also put forward the definition of privacy that to this day is used most frequently; namely, the definition of privacy as the right “to be let alone” (p. 205). They saw this right to privacy as one part of a larger right to be let alone, which includes such rights as not to be assaulted, beaten, imprisoned, maliciously prosecuted, and so forth. Although such privacy is a basic right that many authors today still recognize (Britz, 1999; Velasquez, 1998), others argue that it is not a basic right protected by the U.S. Constitution. While this argument was developed in the U.S., similar views of privacy can be found in most countries, usually codified by law. In some areas, notably the European Union, the recognition of privacy goes beyond the negative right to merely be left alone and extends to the positive right of informational self-determination. In the European Union, privacy is recognized expressly as a fundamental human right (European Union, 2000, Article 7). For now, however, we will continue to use the definition of privacy as the right to be left alone, because this can be viewed as a generally acceptable minimum standard.

Albeit widely recognized and generally understandable, this definition produces several problems. First, it is based on a natural rights approach that is hard to justify. Second, it is too broad to be of much practical use and does not capture all of the meanings of the term that can be found today. The meanings of privacy cover a diverse range from privacy as a situation, a right, a claim, to privacy as a form of control or a value (Gavison 1995). Privacy is interlinked with freedom and property. It can be defined in part as “the freedom to do things away from the eyes and ears of others” (Weckert & Adeney 1997, p. 76). Privacy is invaded when “individuals are unable to control their interactions with the social and physical environment” (Culnan 1993, 344).
There are different reasons why privacy has gained importance over the last decades. The first one, which is probably the most important in the context of this chapter, is the impact that information and communication technology (ICT) has. ICT has not changed the fact that data about persons are collected, processed, and exchanged. However, it has changed fundamentally the speed and scope in which this can be done. It has changed the mobility of data; as Moor (2000) puts it, ICT has “greased” the data. The result of this is that on the one hand, more data than ever before are collected on individuals, while on the other hand, these individuals have less control over what happens with these data than ever before. The availability of ICT also facilitates the creation of synergies and the exchange of data in ways that have the potential to affect people’s lives deeply. One example might be genetic data that can be used to create information about health risks. This could be linked to employers’ or insurance companies’ databases with the effect that individuals lose their employment or are unable to acquire insurance coverage. Such examples easily can be continued, and they show that privacy has a deep impact on the role of individuals in society, on rights and obligations, and on the way we interact on ethical matters. This is why privacy is such a frequently discussed topic in computer and information ethics (Anderson et al. 1993; Johnson, 2001; Mason, 1986; Robison, 2000; Straub & Collins 1990).

The technological development is linked and propelled by economic interests, and, as the previous example shows, the two combine to exacerbate the privacy problem. While traditionally the state has been seen as the greatest threat to privacy, especially in totalitarian states, today many authors see a bigger threat coming from private enterprises that have the technical means and the economic incentive to collect data and that are not regulated in the way actions by state and government bodies and representatives often are (Himanen, 2001; Tavani, 2000). Again, this is not an entirely new development. The original American legal codification of privacy by Warren and Brandeis already aimed at curbing commercial interests that promoted the technical threats to privacy. However, in modern, information-based economies, the incentives to collect data on individuals are great, and regulations are diverse and frequently contradictory. One other reason why the question of privacy is so complex is that it runs across several societal fault-lines; it interferes with the grand discourses of liberalism versus collectivism, freedom, and autonomy; and our societies do not seem to be able to agree on a position with regard to these questions (van den Hoven, 1999).

Justifications of Privacy

Among the different strategies used to defend a right to privacy, one can distinguish between absolute and relative ones. Privacy as an absolute right or value is based on the assumption that it is a basic right comparable to human rights, which must be defended independent of specific circumstances. Privacy
is thus afforded the same status that human rights generally have, and some authors believe that it, indeed, is a basic human right (Rogerson, 1998; Spinello, 1997). Moor (2000) offers a similar distinction by introducing intrinsic and instrumental values. Intrinsic values are those that deserve to be defended, whereas instrumental values are only valuable with regard to something else, ultimately with regards to intrinsic values. One example of privacy as an intrinsic value is put forward by Milberg et al. (1995), who see it as a “hypernorm”—a moral rule that seems to be a human universal and that is generally recognized and does not need further justification. (For a description of the idea of hypernorms, see Donaldson & Dunfee, 1999)

Those authors who do not see privacy as an intrinsic value or as a basic human right and who still agree that it is something worth protecting must show reasons why it is, nevertheless, important. There are again two possible strategies that can be found in the literature for doing so. On the one hand, privacy is defended as important for the individual; on the other hand, it is portrayed as crucial for society. To some extent, these strategies reflect a deontological and a teleological ethical argument, respectively.

The individual approach emphasizes the importance of privacy for the development and maintenance of the individual. Privacy has been described as the “basis for self-determination, which is the basis for self-identity as we understand it” (Severson, 1997, p. 65). That privacy is important for individual development is in little doubt. Just why and how privacy is needed to become a fully developed individual or person is less clear. There seem to be different functions that privacy has in the process of developing individuality. Johnson (2001), drawing on Fried, believes that friendship, intimacy, and trust need privacy in order to develop. The generally shared assumption is that in order to develop satisfactory relationships with others, one must have a place where the other cannot follow, where one is sure to be alone. Without this type of control over who has access to us and who knows what about us, we have difficulties developing meaningful relationships (Rachels, 1995). One problem of the intrusions of privacy through ICT can be that others not only have access to areas that one may believe to be intimate, but they also have more information about individuals than the individuals have themselves (Robison, 2000). In extreme cases, the access that others can have to one’s information is presumed to be enough not only to undermine one’s relationships with others, but also, in fact, to jeopardize the identity or the inner self of the person in question (Brown, 2000). Another aspect of privacy and the individual is that respect for the privacy of others can be interpreted as respect for the other, per se; or, put negatively, a lack of respect for privacy equals a lack of respect for the other (Elgesiem, 1996). For proponents of these arguments, privacy is an instrumental value. However, its importance for the intrinsic value behind it (i.e., personhood) is such that it seems to become an intrinsic value itself. This means that it deserves being protected as a basic right (Introna, 2000).
The other strand of arguments used to defend privacy as an instrumental value aims at its social utility. In this line of reasoning, privacy is seen as valuable for something that is useful from a social or societal point of view. Classically, one can find the contention here that privacy is necessary for the collective deliberation process that determines decision making in democracies. Johnson (2001), for example, states the case that individuals who are constantly observed are incapable of the essential processes necessary for democracy to work. In a more general sense, privacy can be seen as part of the values that characterize democratic societies. Privacy, in this respect, is an instrumental value, because it contributes to the success of democracies (Gavison, 1995).

**Limits and Problems of Privacy**

Independent of the arguments used to defend privacy, most authors agree that there are limits to the right and the protection of privacy (Britz, 1999). “Privacy is a relative concept. It is a continuum” (Introna, 2000, p. 190). This can be explained easily by looking at the two possible extremes of privacy—complete privacy and complete lack of privacy. A complete lack of privacy would lead to social and psychological problems explained by our apparently natural need for an undisturbed space. However, if this space is brought to the opposite extreme—complete privacy—the results would be equally negative. Social institutions rely on information about the members of society. Complete privacy would bring about a collapse of many social institutions (Gavison, 1995), especially those institutions that exert constraints on people, such as military conscription and the tax system. The resulting collapse of much of what defines our societies would be hard to justify on the grounds of privacy protection.

Basically, we find ourselves now in a situation where the value of privacy is recognized, but where it is quite unclear how this translates into specific privacy protection measures. In the context of this chapter, it is important to note that privacy is a moral notion that can be defended from most ethical viewpoints. Many of the defenses of privacy discussed are based on utilitarian grounds. Privacy protection is supposed to increase the individual’s utility by allowing the individual to develop his or her personality to the maximum and to engage in meaningful social interaction. At the same time, privacy maximizes social utility, first by increasing individual utilities and second, by facilitating social interaction. However, privacy can be justified just as easily by deontological arguments. One can see privacy as an intrinsic value, which could be translated into the duty to respect it. Another strategy would be to stress the importance privacy has for allowing the development of individual autonomy. Personal autonomy is important from a deontological perspective, because it is the basis of setting one’s own norms, which, in turn, is a central idea in Kantian (Kant, 1995) morality. Privacy has a moral value, because it can be seen as a sign of respect for persons, which again can be justified by teleological (i.e., aims-base, consequentialist) as well as deontological (i.e., duty-based) ethical theories. Furthermore, respect for pri-
Privacy also can be seen as a virtue, which puts it squarely into the realm of virtue ethics.

Privacy is thus a moral value or a moral right, and it is worth defending. However, like most moral rights and values, it is not absolute. Philosophical ethics have always had to deal with the question of how to limit moral rights and what to do in case of a conflict of different rights. In many cases, moral rights deemed significant within society are transformed into legal rights. Privacy is no exception. The question of the limits of a moral right then becomes the question of the limit of a legal right. While this sort of question often is solved more easily in practical terms, due to the existence of a hierarchy of courts that gives us practical solutions, privacy still raises a lot of questions when one looks for its exact extent and limits.

Some of the limits of privacy are fundamental and closely related to the justification of the term. If privacy gives individuals freedom to interact and to do what they want without detection, then it also gives them freedom to do undesirable things (i.e., commit crimes, do terrorist acts, etc.). Levy (1995), therefore, can ask whether we can protect our privacy in an age of computers “without also protecting the dark forces in society” (p. 652). A somewhat less apocalyptic problem that can be raised by privacy is that of intellectual property. Some authors suggest the framing of privacy in terms of property. That means that information about a person is seen as that person’s property, and, consequently, the person gets to decide what to do with it (Hunter, 1995). Unfortunately this does not solve the problem either, because it remains questionable whether personal information can be described usefully in terms of property, and, even if this were agreed upon, it would change the problem to the question of the limits of personal property.

Apart from these fundamental problems that most individuals would be hard-pressed to address, there are also many practical problems with privacy protection. We have seen that privacy can be described as a right, but the status of the right remains open. Is privacy a moral or a legal right, and what is the relationship between the two? In most societies, a right to privacy is recognized by the legal system, either explicitly or implicitly. However, as soon as we enter the sphere of legal rights, we are confronted with a whole new set of problems. Given the international nature of the information technology that threatens privacy, we find a host of international questions such as jurisdiction and cultural and language difficulties. One problem in this regard results from the different perceptions of privacy between the U.S. and Europe. These differences go deep enough to endanger data exchange between the two areas (Langford, 1999; Tavani, 2000). The EU follows a strong privacy protection regime and outlaws transborder data exchange with countries that do not guarantee the same level of protection. Given that the U.S. has weaker privacy protection, complicated arrangements have been set up to facilitate data exchange.
Having now discussed the ethical aspects of information assurance, privacy, and their justifications and limits, we can proceed to the difficult question of their relationship with regard to ethics.

The Relationship of Information Assurance and Privacy from and Ethical Viewpoint

Information assurance and privacy can reinforce one another, but they can also come into conflict. This section will discuss these two possibilities while emphasizing the way in which this may affect moral rights or obligations.

**Ethical Correspondences of Information Assurance and Privacy**

Information assurance and privacy can correspond and thereby jointly protect or even constitute moral values. Both terms can refer to the concept of security. Information assurance in this text is understood as the attempt to increase the security of the use of ICT on different levels. This more technical view of security can be seen as a precondition of a more personal psychological concept of security. Human beings need security in an emotional sense, which means that they need to feel secure. Technical and personal security can support this feeling of security, but they do not have to be. One can feel secure because one is not aware of the danger, and one can feel insecure despite an “objective” lack of threats. However, objective technical security can be translated easily into personal security. Most people will feel more secure in a modern car with all sorts of active and passive security measures than in an older one that lacks these measures. Similarly, information assurance is a precondition for feeling secure when interacting with computers (Spafford, 1995). It is this feeling of security, this psychological security, that was cited as one of the main reasons that privacy should be defended. Security, therefore, is probably the most important area where information assurance and privacy overlap, and where, at the same time, they protect an important moral value—the individual and its formation (Moor, 2000). Drawing on Giddens and Goffman, Brown calls this a “‘protective cocoon’ which allows individuals to deal with life on a daily basis and protect the inner self they know from exposure to outside scrutiny. This ‘veil’ separates self from those things that are external and therefore not self, in this manner providing the most basic sense of ontological security” (Brown, 2000, p. 63) Technical security is thus necessary to produce privacy. An example would be so-called privacy-enhancing technologies (PETs), and the most fundamental of these is encryption, which simultaneously promotes privacy and security (Tavani & Moor, 2001).

A related area where privacy and security work to achieve a shared goal, which is generally recognized as an ethical value, is that of trust. Many authors emphasize that in order to develop trust, an individual needs physical security as well as privacy. Again, this is based on assumptions about the working of the
human mind, which needs a feeling of security and a feeling of individuality in order to interact meaningfully with others (Koehn, 2001). The dependence of trust on privacy and security is a prevalent topic of discussion in e-commerce. A lack of trust has been identified as one of the major impediments to the continued success of online trading. Many individual customers are reluctant to buy or sell online because they do not trust the procedures. The reasons for this are manifold, but most authors agree that they can be found at least partly in the areas of security and privacy (Hoffman, Novak, & Peralta, 1999; Nikander & Karvonen, 2000; Khare & Rifkin, 1998).

Another angle under which the affinity of privacy and security can be captured is that of control. For individuals to be in control of their lives, a certain amount of control over what is happening to them and with them is indispensable. This control can be interpreted in terms of security, which means that the individual can prevent unwanted intrusion. This sort of control then automatically entails a degree of privacy (Camp, 2001). Again, control in this sense can be seen as a moral value, because it is a sign of the autonomy of the individual that we have identified as ethically important.

*Ethical Contradictions of Information Assurance and Privacy*

While security and privacy can overlap, as we have seen in the last section, they also can be contradictory. As a general point, one can note that security requires openness, clarity, and accountability, whereas privacy often means the opposite (Beu & Buckley, 2001). Privacy and security can come into conflict in different areas. One example that can be used to demonstrate the possible contradiction is trust. While we have argued that trust requires privacy and security at the same time, the relationship also can be contradictory. One argument along this line is that security can limit the exchange of ideas, and that this free exchange is one of the basic building blocks of the computer community. An increase in security thus means a decrease in free speech and consequentially a decrease in trust (Rotenberg, 1995). Other authors argue that the entire trust issue is misleading, because it is based on fallacious premises. A large part of the literature on trust in e-commerce, for example, tries to show ways that can be followed in order to build trustworthy information systems. Critics of this approach argue that one cannot trust technology; one can only trust people. More security, therefore, cannot induce trust (Rutter, 2001; Corbato, 1995).

Another area where security and privacy may be contradictory is that of power. Especially with regard to hierarchical organizations, both of these terms can be seen as an expression of power of particular groups or individuals. In this setting, security usually means control over access and use of systems, and in many cases, this will be in contradiction to the power to protect one’s privacy (Forester & Morrison, 1994). The expression of such conflicts often can be seen in more technical issues that are needed to implement security or privacy.
concerns. Examples of this are biometrics or encryption. Both of these technologies increasingly are used to secure data and information systems, and both also can be interpreted as tools that have the potential to decrease privacy. While biometrical protection of one’s personal data and files may increase one’s privacy, it also can serve to identify a person more clearly and to use this data for other purposes (van der Ploeg, 2001).

The most important area of conflict between security and privacy, however, is that of surveillance, especially the surveillance of employees by organizations. All of the arguments mentioned in this section apply to this, but the topic acquires its importance due to the sheer magnitude of surveillance in today’s societies. While there are important national differences in this area, it is probably true to say that most commercial organizations have rather strong incentives to subject their employees to surveillance, and the practice is widespread (Hartman, 2001; Schulman, 2000; Bowie, 1999). The reasons for this differ among companies, industries, and countries, but most of them have something to do with information assurance. The rationale for surveillance usually is to produce security for the company in some sense, be it for legal problems (Brown, 2000), competition, or other economic considerations such as making sure that employees do their job (Boncella, 2001; Posner, 1995). The price to be paid is a decrease in employee privacy. It is in this situation—the surveillance of employees in their workplaces—that the problematic relationship between security and privacy becomes most clear, and the question of ethical problems and of individual decision making is most salient. It is, therefore, a good starting point for the discussion of how these questions can be addressed. Since the proposed solution in this chapter is the concept of responsibility, we now will look at how individuals can make responsible decisions regarding the tension of privacy and information assurance.

**RESPONSIBILITY AS AN ANSWER TO ETHICAL PROBLEMS**

So far, this chapter has argued that security and information assurance and privacy are terms with important ethical aspects, but that their relationship is problematic. Individual and organizational decisions with regard to the two concepts will affect people’s rights and obligations in most cases, but it is usually unclear exactly how this will be the case. The ethical evaluation of such decisions depends on a highly opaque muddle of ethical theories, moral practices, empirical consequences, legal frameworks, international negotiations, and so forth. One ethical concept that is used frequently to address such muddles is responsibility. This section will describe briefly the concept of responsibility, emphasizing the individual perspective. By concentrating on the conditions of responsibility, it will
be shown that responsibility, while in principle very useful for this sort of situation, requires more than an individual is able to deliver.

The Conditions of Responsibility

It will not be possible in this chapter to present a comprehensive overview of the concept of responsibility and its use in moral philosophy. (For more exhaustive theories of responsibility, see Bayertz, 1995; Fischer, 1999; French, 1992; Lenk, 1998; May & Hoffman, 1991; Neuberg, 1997; Paul et al., 1999; Sänger, 1991; Stahl, 2004.) The discussion, therefore, will concentrate on the subject of responsibility and the conditions a potential subject needs to fulfill in order to be admissible as a subject. In order to do this, it will be necessary to give a brief definition of the concept of responsibility.

In this chapter, responsibility will be understood as a social construct that results in the ascription of an object to a subject, usually before an authority of some kind. The most accessible example of this is the case of legal responsibility, where the object is the crime, the subject is the accused, and the authority is represented by the law and the judge who interprets it. Responsibility, understood in this way, is a complex notion that, in order to be practically relevant, requires attention to many details such as the acceptability of the underlying rules, the temporal aspect of ascription, and the admissibility of the object. There are several advantages to the concept of responsibility over other normative constructs that let it appear as a suitable candidate to address the problems raised by information assurance and privacy. Responsibility is a formal process that can transport different meanings. That means that it is capable of addressing the legal questions at the same time it deals with the moral and ethical ones. Furthermore, responsibility, at least in its legal form, is well established. It also has a positive image, and responsibility statements often are more acceptable than other moral assertions.

The most important component of the responsibility ascription is the subject. Traditionally, the subject has been the individual adult and rational human being—the person. In order to be ascribed responsibility, the subject needs to fulfill several conditions. The one that probably is most frequently named is that of causality. In order to be ascribed responsibility for an object, the subject must have a causal relationship with it, must have caused it or at least have been capable of changing the course of events that led to the object (Bechtel, 1985; Birnbacher, 1995; Etchegoyen, 1993; Goldman, 1999; Jonas, 1984; Zimmerli, 1987). This causality assumes several other conditions. In order to be able to influence events, the subject must have knowledge of the consequences of actions (Rötzer, 1998) and must have the power to change them (Lenk & Maring, 1990; Nida-Rümelin, 1998; Staddon, 1999). In order to be able to do this, the subject needs to fulfill some more implicit conditions such as freedom (Höffe, 1995; Frankfurt, 1997; Wunenburger, 1993) and personal qualities such as
emotions, empathy, a certain amount of rationality, a certain state of mind, and so forth (Bierhoff, 1995; Hart, 1968; Stocker, 1999). Some of these assumptions and conditions are quite difficult to come to terms with, as the example of the concept of freedom shows. Freedom is a highly contentious topic in philosophy, and it is not clear exactly what it is, whether it is possible, and how it relates to responsibility (Wallace, 1996).

The Limits of Individual Responsibility in Privacy and Information Assurance

The previous discussion of the conditions of responsibility should have made it clear that it is very hard for an individual, as the traditional subject of responsibility, to live up to the expectations, even in rather simple cases. While humans usually fulfill the personal qualities such as awareness, intentionality, and emotions, they are hard pressed fulfilling all of them simultaneously. In the context of complex sociotechnical systems that are the center of attention in this chapter, individuals generally fail to have the necessary knowledge, freedom, and power to change events. They may play a role in the causality but are often unable to change causality, even if they are aware of them. This has led to a weakening of the role of the individual as the subject of responsibility, and even to the perception that there is a loss of the subject (Hubig, 1995a; Hubig, 1995b; Kaufmann, 1992).

In order to clarify the difficulties that individuals have as subjects of responsibility, let us return to the problem at hand, which is ethical responsibility for information systems with regard to security and privacy. Let us take a look at one typical example of this—a manager who has to make a decision regarding the introduction of a system that monitors employees’ Internet use. In order for the social construct of responsibility ascription to be successful and acceptable, the manager would have to fulfill the conditions. First, the manager would have to play a part in the causal chain of events. This condition is met due to the realities of the case. Second, the manager would have to possess the freedom to influence events according to his or her own free will. Disregarding the philosophical problems of freedom and free will, we will grant this. By definition, the manager also does fulfill the third set of conditions; namely, those referring to personhood. Unfortunately, however, the manager lacks the remaining capabilities that would render him or her a suitable responsibility subject. In order for the manager to be a proper subject, the manager would have to know the situation well enough to estimate all of the relevant factors and developments. This is practically impossible since the manager does not know all of the stakeholders’ views, which is principally impossible because the development stretches into the unknown future.

Furthermore, the manager not only would have to know the objective facts, but also would have to know their normative evaluation. That means the manager
would have to know not only the laws but also the moral norms of the affected parties, and the manager would have to know how to interpret and reconcile these in case of a conflict. This discussion of the complex ethical relationship between security and privacy has shown that the knowledge necessary to be a competent subject is complex and distributed. It seems quite impossible for any one subject to have it at his or disposal. But even if it were available, it would be impossible for an individual to reconcile all of the potential contradictions and feedback loops and to come to a decision that is responsible in the sense that it is sustainable and attributable to the individual. If this is true, and if individuals, even under the best of circumstances, will not be able to act as subjects of responsibility in light of the ethical problems of security and privacy, where does this leave us?

**WHAT ABOUT THE END USER?**

The purpose of this chapter is to show that information assurance and privacy are concepts of high ethical importance; their relationship with each other and with ethics is highly complex. The chapter analyzed the theory of responsibility and argued that, despite some advantages of the notion, it runs into serious difficulties when applied to the complex ethical questions relating to privacy and information assurance. The one specific problem that was discussed in more depth was that of the individual subject of responsibility. It was argued that an individual lacks some of the crucial conditions necessary for a successful ascription of responsibility. This allows us to give an answer to the question posed in the title of the chapter: The combination of information assurance and privacy is something that cannot be addressed successfully by individual ethics, at least not by individual ethics as expressed by the concept of responsibility.

Where does all of this leave the end user who reads this chapter? There are different possible answers to this. The message of the chapter should not be misconstrued as meaning that there is no place for individual responsibility in the normative muddle of security and privacy, and it also should not be misunderstood as a blanket excuse for individuals to do as they like. Given the severity of the problem and its importance for organizational and social life, however, the chapter leads to the conclusion that it would be irresponsible to rely on the individual, who is not equipped to deal with questions of this sort. The argument in this chapter, therefore, can be used by end users as an explanation of their incapacity to accept individual responsibility for the complex social relationships within privacy and information assurance. Going back to the example of the manager who is asked to introduce a surveillance system for Internet use, a manager could use this chapter to demonstrate his or her limits in the capacity as a responsibility subject. This does not mean that the manager should go back to his or her manager and refuse to do the job. Instead, the reflection on the
concept of responsibility would allow the manager to clearly state what he or she is capable of doing and not doing. Furthermore, it would allow the manager to indicate a way of dealing with the problem. Realizing the manager’s lack of information about the affected people’s views of norms regarding Internet use, the concept of responsibility introduced here would provide a framework for determining how to get this information. This means that the manager might devise specific or new processes that would allow the retrieval of the information. In this way, the manager might meet the expectations or requirements of information assurance as well as privacy considerations.

This raises several other issues. If the analysis of the problem is correct, and if ethics is involved in our topic, then the individual is not a promising starting point from which to look for solutions. Thus, we have to ask how the problems can be addressed. This question aims at directing the reader’s attention to the idea of collective responsibility. I believe that the concept of responsibility offers the promise to be able to address the problem. This would be possible by transcending the traditional definition of the individual human being as the sole possible subject and by allowing more complex and collective ascriptions. This approach raises several new questions (e.g., whether collectives can be moral subjects), but it allows for the extension of the term. While individuals generally lack power and knowledge in complex situations, the same is not necessarily true for collectives. This argument for the extension of the concept of responsibility has been made before (French, 1992; Werhane, 1985) and, in some respects, is generally recognized already. If we were to agree that it is possible to address the ethical problems of security and privacy by extending the concept of responsibility, this again would raise many new questions and require us to collectively agree on the applicable norms, the problems in question, institutions of ascription, and sanctions.

Again, this is an area where the individual end user is concerned. If collective responsibility is to be successful, then even a superficial view indicates that it is to be connected with individual responsibility. It will be the responsibility of individuals to participate in the discourses and processes that define suitable collectives as subjects as well as potential sanctions, or mechanisms of attribution. Furthermore, there must be a structure that allows the drawing of conclusions from individual to collective responsibility and vice versa. All of these are aspects that individuals should keep in mind, and where end users can and must play a central role.

The essential message of the chapter is, thus, that individual responsibility plays an important role in the relationship of information assurance and privacy. At the same time, it cautions that concentrating exclusively on the individual as the responsible agent is easier than going down the long and stony way to collective responsibility but, as I have tried to show in this chapter, is not very promising and, thus, irresponsible.
REFERENCES


Boncella, R.J. (2001). Internet privacy—At home and at work. *Communications of the Association for Information Systems, 7*.


