

# Privacy and Security as Ideology

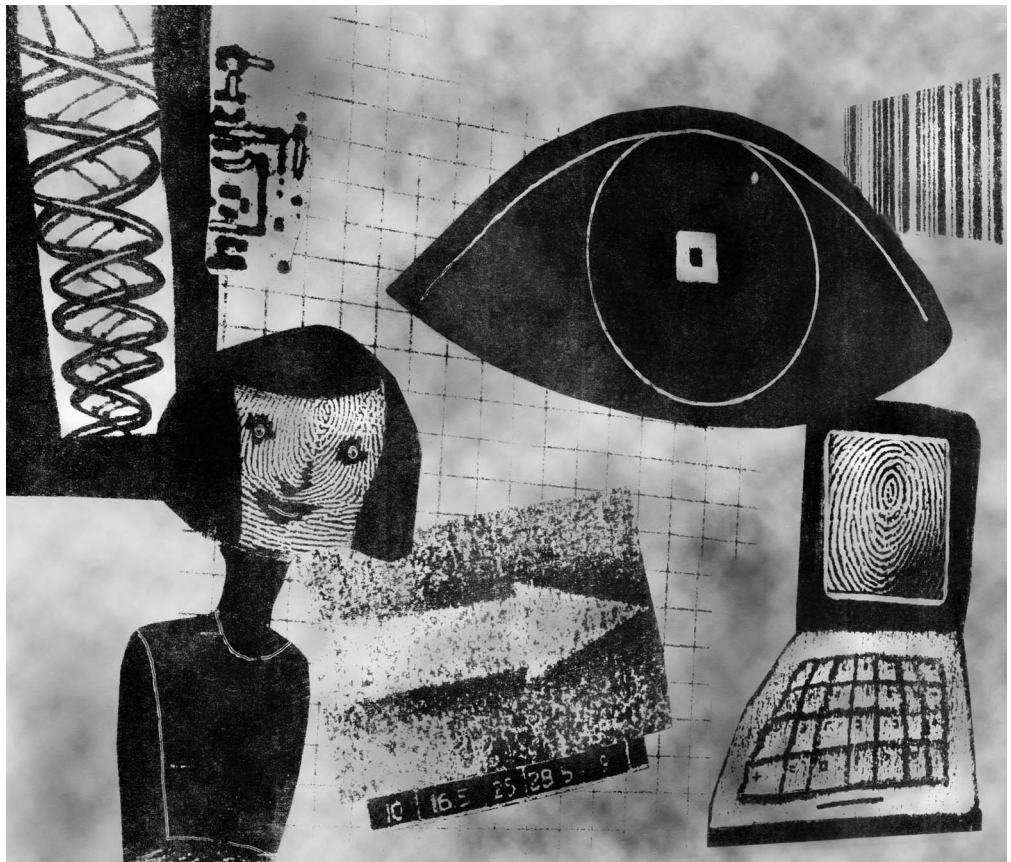
BERND CARSTEN STAHL

Privacy and data protection are among the prime problems of the information society. Many of us are concerned by the fact that electronic data about us can be used for purposes beyond our control. Privacy therefore has a close relationship with security. If data about us is not secure then this can threaten privacy. This line of argument suggests that privacy requires security. A somewhat contradictory argument would be that, in order for security to be guaranteed, we need to limit privacy. If all information about everyone were known, then security threats would be much easier to address and sanction. In this scenario, privacy and security seem to be mutually exclusive. This confusing and contradictory starting point for a discussion of the relationship between privacy and security is exacerbated by a number of aspects. It is not really clear what constitutes privacy, nor do we have a generally agreed-upon def-

inition of security. There is also no agreement on how these two concepts are to be protected (by ethics, the law, markets, or other mechanisms) or who should assume

responsibility for them (the state, the individual, organizations, etc.) [62].

Briefly, the intersection of privacy and security is a conceptual muddle and consequently characterized



©GETTY/STOCK ILLUSTRATION PF

by policy vacuums. For this reason [39]-[43], as well as because of the importance the issue has for our individual and social existence, privacy and security can be viewed as ethical questions. At the same time the privacy and security area attracts a large amount of attention from the

dence of the ideological use of the terms privacy and security.

Overall, this article will offer a novel viewpoint of the intersection of computer and information ethics and commercial practices. The use of critical theory has the advantage of offering an estab-

integral part of philosophy, has been formally discussed since the ancient Greeks. As part of the normative constitution of the social world, it predates philosophical discourse and permeates in all areas of social interaction. Here, I will follow what has been termed the “German tradition” of moral philosophy [63], which distinguishes between morality as the factually accepted norms that guide individual and collective behavior, and ethics as the theory and justification of morality.

Moral rules are those that agents follow because they represent what is good and right. Examples of moral rules could be an obligation to help the needy or an interdiction of downloading proprietary software. Ethical theory explains why moral rules are desirable. It can draw on a rich history of justificatory ideas ranging from duty (deontology) to utility (teleology) to the individual character (virtue ethics). It is not the purpose of this paper to engage in the ethical discourses surrounding privacy and security but only to demonstrate their relevance by explicating some of the more frequently used arguments.

### **Ethics of Privacy**

Privacy is generally acknowledged to be a (moral) good [72], but there is less agreement on what exactly it is or why it is valuable [22], [58]. Historically, privacy concerns go back to the ancient Greeks [52], but only acquired legal recognition towards the end of the 19<sup>th</sup> century [59], when the most widely spread definition of the term as the “right to be let alone” was coined by Warren and Brandeis [70]. This definition is still used today [5], [67], but it lacks the clarity needed for a thorough investigation. Privacy can refer to control of information, social control [13], to perceptions and psychological states [67], to rights and obligations, to personal curiosity or social structures.

## **Privacy is generally acknowledged to be a (moral) good, but there is less agreement on what exactly it is or why it is valuable.**

commercial sector because it has the potential to determine the success or failure of many business ventures, most obviously e-commerce activities. The location of privacy and security on the fault line of a variety of discourses is one of the reasons for some of the problematic use of privacy and security concepts. Privacy and security are often described in terms of ethics and therefore taken to be of an ethical nature. At the same time, they are used by commercial organizations to promote their particular, usually financial but often also political, objectives. This is problematic because the commercial use of the terms privacy and security promotes a particular ideology and uses the ethical recognition of the concepts to limit critical discourses.

This article will use a critical approach in the tradition of Critical Theory and its developments in Critical Research in Information Systems (CRIS) to expose and overcome these discursive closures. I begin with a review of the literature on privacy and security, which will support the contention that these are ethical concepts. The concept of ideology and critical research will then be discussed. This will lead to a critical discourse analysis of a text from a commercial software vendor, which will provide empirical evi-

lished perspective on ethically difficult practices. The methodology of critical discourse analysis should be of interest to individuals from a technical background because it facilitates the generation of insights that are different from most technical research. Critique of the practices and rhetoric of large commercial software vendors is not novel *per se*. This article is nevertheless a valuable contribution because it uses a different theory and methodology and therefore provides new arguments for separating the ethical and commercial uses of the concepts of privacy and security.

### **Ethics of Privacy and Security**

There are discourses concerning privacy and security that focus on the ethical quality of the concepts where the resulting ethical connotation of the terms is used to promote particular interests. A brief review of the literature on privacy and security, emphasizing the ethical angle of the arguments, will help to illuminate this point.

There are two main difficulties to this approach: First, the debates on privacy and security are individually too extensive to be captured comprehensively in a brief section. Second, the concept of ethics is difficult to get a handle on. Ethics, an

What is probably beyond doubt is that the current interest in privacy is related to the use of information and communication technology (ICT). ICT arguably does not cause the collection and (potentially unwanted) use of data but in many cases it facilitates such uses [2], [31]. Privacy has thus been identified as one of the major ethical issues in ICT from the early days of the debate on computer and information ethics [38] but also in information management [65]. The use of ICT thus leads to a change of the understanding of privacy [51]. As a result of the challenges of privacy, a variety of legal instruments have been developed by different countries [11].

What is of interest in this article is the ethical nature of privacy. This can best be observed by looking at the arguments proposing or justifying a right to privacy. Privacy can be seen as an absolute or a relative right. Where it is perceived as absolute this means that it requires no further justification. It is then comparable to a natural right, something that is irreducible [61]. Privacy can obtain the status of a human right, which is reflected by the right to the respect of privacy as developed in Article 8 of the European Convention on Human Rights. This justifies Rogerson's [52, p. 22] reference to privacy as a "fundamental right". However, some authors do not see privacy as absolute but relative, which means that it needs to be justified with regards to other values or rights. This distinction mirrors the one between privacy as an intrinsic or instrumental value [43], [66]. Both sides of the argument agree, however, that privacy is a moral good. What they disagree on is the ethical justification and therefore the reach of the concept.

On the individual level privacy is often described as a necessary condition for healthy personal development. We require privacy

to become autonomous and independent humans who are able to interact with others and create rewarding and useful relationships. Respecting privacy is thus an expression of the respect for the autonomy of others [7], [16], [29], [31], [50], [58]). Since a society of incomplete individuals

There are different areas and topics of security ranging from national and military security to the security of one's personal belongings. The topic of this article, computer or information systems security, can have an influence on many of the other aspects as well. There are general defini-

## Privacy has been identified as one of the major ethical issues in ICT from the early days of the debate on computer and information ethics.

cannot function, privacy can also be justified by social considerations. Privacy not only allows us to develop healthy interpersonal relationships, it also seems to be required for democratic states to function [22], [31].

This brief characterization leaves open many questions. It does not address questions of the legal status of privacy nor the exact limits of this perceived right, or ways of adjudicating conflicts between privacy and other rights. It leaves open, for example, the issue whether, or under which circumstances, workplace surveillance is justified [61]. These shortcomings are not problematic for this paper because the point of the discussion of privacy was to show that the concept is of an ethical nature. It is recognized as a moral value, which can be justified using a variety of ethical arguments ranging from utilitarian considerations to issue of virtue and deontological arguments. Having thus established the importance of ethics in the discourse surrounding privacy, we can proceed to look at ethical aspects of security.

### Ethics of Security

Security, at least with regards to computing, seems to be a more straightforward concept than pri-

tions, such as the classical one by Landwehr [36, p. 2], which states that a system is secure "if it adequately protects information that it processes against unauthorized disclosure, unauthorized modification, and unauthorized withholding (also called denial of service)."

Unfortunately, the text goes on to say that no practical system can achieve these goals simultaneously and that security is inherently relative. In an earlier paper Landwehr [35] points out that even in strictly structured social systems such as the American military, security is never unambiguous.

Security is thus similar to privacy in that most people think that it is important but they find it more difficult to agree what actually constitutes security [1] and why it is important. Security has an economic aspect [9], but its importance goes far beyond financial considerations. Security is important for all of us individually but, given the lack of agreement on the concept of security, there is no generally accepted behavior that would express security concerns and it has been argued that people act inconsistently or self-contradictorily with regards to security [44]. Berendt *et al.* [4], for example, discuss a study which seems to indicate that users voice different preferences with regards to

security and privacy from the ones they actually act upon.

The main question of interest here is whether and in what way security can be seen as an ethical concept. One main argument for the

recognized as being important ethical issues of markets [21].

On a more general level, as Nissenbaum [45] argues, the question of the moral quality of security can be described in terms of the harms

security are notions with moral content and ethical justification, we will now briefly discuss their relationship. When looking at the use of the concepts in a commercial environment it will be important to know how they relate to each other.

Given the complexity and many facets of both concepts involved, there is no clear and unambiguous description of their relationship. The literature shows examples of different conceptualizations of the link between privacy and security. In some respects, most notably from a law enforcement view, they are contradictory. Individual privacy preferences, where they involve criminal activity, will go counter to security needs. There is a wide variety of legal activity on both sides of the Atlantic, ranging from the U.S. Patriot Act to the European Convention on Cybercrime which bear testimony to this. Governments everywhere are tempted to limit privacy rights in order to promote security considerations [20].

At the same time, one can argue that privacy and security overlap and reinforce each other. On the level of the individual user, security can be seen as a precondition of privacy because a lack of security may allow unauthorized access to data, which, in turn, will jeopardize privacy. But even in the field of criminal activity it has been pointed out that decreased privacy can lead to a decrease in security because guarding privacy via anonymity allows some individuals to interact with the police and give tips, which they might not do if their identity were known [58]. Another reason for overlap of the concepts is that they both have to do with control, with strong control of personal data apparently equating to privacy as well as security [8]. There are several technologies that can be used in this sense that support privacy as well as security. These include encryption [65], so-called privacy-enhancing technologies (PET) [66], and anonymizing technologies [8].

## On the individual level, privacy is often described as a necessary condition for healthy personal development.

moral quality of security is that it seems to be a psychological need, which Giddens [23, p. 50] terms “ontological security.” Security is thus important for the ability to interact with others in a self-confident manner. It is also required to develop relationships of trust with others [68].

A main argument for the moral quality of security is thus based on individual needs and perceptions as well as the impact of security on interaction. However, there are also aggregate issues of security that have a moral side. Security in computing is a major cost factor with estimates of overall cost of security (or lack thereof) varying widely but always ranging in the billions of Dollars, Euros, Pounds etc. Such costs are of course a moral issue from a utilitarian point of view and they also prevent society from investing these resources in other worthy causes. Security issues also play a large role in computer crime and digital forensics. The ubiquity of computing in modern society renders it an important ingredient of many types of crime [69]. Hacking and viruses are a major concern. Apart from the economic issues they raise, they are also related to criminal activities and breaches of criminal law are generally viewed as being morally problematic. Another moral issue on the social level is that security can be seen as an externality [10]. Externalities (and public goods) have long been

that its infringements would constitute. This leads her to an interesting discussion of two types of security related to computing: Technical or individual security and political or social security. Nissenbaum argues that these two are often conflated even though they are fundamentally different and require different technical or political solutions. Drawing on the Copenhagen School, she discusses the concept of “securitization.” Securitization stands for the depiction of a possible risk in terms of a fundamental threat to an important entity, most often the nation state. The securitization of a risk means that it becomes a moral imperative to protect the entity in question. This implies a strong moral standing of security that overrides opposing concerns. Nissenbaum argues that computer security has been securitized in particular following the 2001 terrorist attacks on New York and Washington. Such securitization leads to possible solutions that are arguably not relevant for individual computer risks such as hacking, viruses etc.

Nissenbaum’s considerations are of relevance to this paper because the process of securitization of computers and ICT contribute to the high moral standing of security that makes it a suitable tool for ideological misuse as discussed below.

### Privacy and Security

Having established that privacy and

This technical overlap of security and privacy can be explained at least partially by the fact that they serve the same moral ends. Both cater to the individual psychological need to feel protected from outside interference. They are part of the “protective cocoon” that facilitates the building of identity [7]. Both are required to build trust [53], and therefore to the establishment of sound relationships [28]. Trust and security are thus mutually enforcing moral goods for the individual, even though an overemphasis on security can also create problems with trust [46]. Security and privacy also lead to social well being and the creation of general utility. Respecting them is a sign of respecting individuals and their autonomy. It is also a sign of a morally good character disposition. The moral value of privacy as well as security can thus be explained by the most important ethical theories from Kantian deontology to utilitarianism and virtue ethics. Having established this much, we can now proceed to look at ways in which the concepts of trust and security are used, which do not necessarily conform to their moral nature.

## **Ideology and Its Critique**

We now embark on an ideology critique regarding the concepts of privacy and security.

### **Ideology**

Ideology is a central concept of critical research in information systems as well as critical research in general. Ideologies limit the ability of the individual to perceive the world and they are therefore counter forces to the main aim of critical research, namely emancipation. By addressing issues of ideology and emancipation, we enter the context of critical research. Critical research has historically developed from Marxism, even though many contemporary critical scholars cannot be called Marxists. What it still shares with

Marxism is a fundamental suspicion of the capitalist ways of organizing production and other economic functions. Critical research in information systems has been developing for at least 20 years. It is often defined as a research “paradigm,” the third one after positivist and interpretive research [46]. Central to critical research is the desire to change social reality and to promote emancipation.

Within critical research the concept of “ideology” plays a central role. Fairclough [17, p. 9] suggests the definition of ideologies as “representations of aspects of the world which can be shown to contribute to establishing, maintaining and changing social relations of power, domination and exploitation.” It is important to see that ideologies are not necessarily falsehoods or based on bad faith [56]. Instead, ideologies are taken for granted, shared conceptualizations, or constructions of (social) reality. The problem is that such constructions will often become reified and taken for absolute truth [39]. These objectified constructions typically hide vested interests and power relationships [27]. Such hidden agendas are problematic when they can no longer be discussed, which is the case when they become recognized as natural “facts.” Ideology therefore makes it harder or even impossible for individuals to reach their full potential. It thus precludes emancipation [26].

### **Ideology of Privacy and Security in ICT**

How can we identify instances of ideology in ICT? If the kind of ideology we are concerned with is the reification of social constructions for the benefit of particular groups, then we need to pay attention to situations where certain groups or individuals are advantaged to the detriment of others. Of particular concern here are such instances where the moral nature of privacy and security

are used to limit discourses with the aim of facilitating gains for certain groups or individuals.

One could thus speak of ideology in cases where one can identify the promotion of, say, security as a moral and thereby universal good in such a way that it privileges certain groups. This is often the case in ICT security, which is frequently designed specifically to protect certain interests, typically those of the vendors and their customers, with little regard to other possible stakeholders. Furthermore, it can even be used more specifically to protect the interests of vendors to the detriment even of their customers, who can be economically locked in [1].

One could argue that such situations are not particularly serious because, in a functioning market, customers could seek different suppliers. They can only do so, however, if they are aware of problematic effects. This is where ideology as reification plays a role. If the state of affairs is perceived as natural and unchangeable, as the result of developments that cannot be influenced, then those who are privileged no longer need to justify themselves for their advantages.

Technology, including ICT, is often used for such acts of reification. If we are told that technology has a certain nature, for example that the Internet is intrinsically democratic, then this need no longer be discussed. Such reification is closely linked to the idea of technological determinism, which assumes that technology has certain properties that lead to determined consequences. Such technologies are then removed from democratic scrutiny [19] and they can be promoted using moral arguments including privacy and security. Pertinent examples of this might be the assumption that the introduction of surveillance technology such as CCTV cameras will lead to a reduction of crime [37] or that the use of ICT in teaching will lead to better educational outcomes [54]. While there is a long tradition of criticizing the idea of technological determin-

ism, it can still be found as a powerful aspect of governing ideologies.

Ideologies are generally accepted social constructions and as such they are based on a shared use of language. Indeed, language is not only the vehicle of ideology, but its essence. When thinking about the relationship of ideology and ICT it is thus important to concentrate on linguistic aspects. Proponents of certain ideological interests often use rhetorical devices to promote their view. A frequently used one is the use of metaphors. Such metaphors, if used successfully, will take on a life of their own and render the originating interest invisible. They can be turned into reifications when they shape the generally accepted definition of technology or its properties. There are several good examples of such use of metaphors as vehicles of ideology in ICT. One of them is the use of the word “virus” for a certain type of self-replicating software. Viruses are generally recognized to be dangerous and undesirable, which renders strong measures against them easily enforceable. It precludes a possible discussion of positive aspects of such programs and thereby furthers the interests of those

who oppose them to the detriment of those who may have legitimate reasons to create them [33]. Another good example is the use of the word “piracy” for the unauthorized downloading of computer programs or digital content. “Piracy,” being originally a horribly violent type of illegal activity, carries the connotation of something not only illegal but highly reprehensible, very similar to the related crimes of murder and rape. The use of the metaphor paints a very clear (and arguably misleading) picture of the activity of unauthorized downloading. Someone committing piracy must be a pirate and hence an evil person. This use of the word thus reifies the moral evaluation of an activity, leads to discursive closure, and thereby promotes the interests of some, namely intellectual property holders, to the detriment of others.

These uses of ideology have many manifest implications. They lead to the hardening of social practices, for example in the intellectual property area. By withdrawing technology from discourse, ideology establishes precedents that become self-reinforcing. One example of this would be a hierarchical information systems development process. There is much

literature suggesting that participative development projects have a variety of advantages from an ethical as well as a business perspective. However, if ICT is seen as fundamentally determined, then there is no need to have users or other stakeholders participate in design decisions. Emancipation cannot become part of the agenda.

### Discourse Analysis as Ideology Critique

In order to answer the question of how ideological assumptions shape discourses on privacy and security and vice versa, it will be helpful to use established research approaches. Here, I use the methodology of critical discourse analysis. There are many different ways of doing critical research. Some of them use social science methodologies, often qualitative ones, to investigate issues of emancipation and power in social settings [3]. The other main group of critical methodologies is aimed at investigating the use of language and its implications for emancipation. Critical discourse analysis (CDA) is part of this second set of methodologies. It emphasizes the identification and exposure of naturalizations, reifications, and discursive closures that pre-empt emancipation. If “lan-

**Table I**  
Guiding Questions to Identify Habermasian Validity Claims (adapted from Cukier *et al.* [14], [15]):

**Truth: Argumentation and evidence**

- T1. What is said about the technology?
- T2. Are the issues and options clearly defined?
- T3. What costs and benefits have been identified and assessed?
- T4. What evidence has been provided to support these arguments?
- T5. Has the relevant information been communicated without distortion or omission?
- T6. Are there ideological claims which are unexamined?

**Rightness / Legitimacy: Whose Interests?**

- L1. Who is speaking, who is silent, what are their interests?
- L2. What is privileged? What is not said about the technology?
- L3. What is assumed or implied?
- L4. What is missing or suppressed in the discourse?
- L5. How are the decisions legitimized?
- L6. Who is involved? Who is not involved?
- L7. What are the stakes and interests involved or excluded?

**Authenticity / Sincerity: Metaphors and Descriptors**

- S1. Do metaphors and connotative words promote or suppress understanding?
- S2. Do metaphors and connotative words create false assurances?

guage is pure ideology” [48, p. 123], then discourse analysis is a natural choice for undertaking ideology critique. It is important to note that it is not the purpose of CDA and ideology critique to overcome ideologies and see the world as it “really” is. Most critical researchers would have serious ontological and epistemological reservations regarding the possibility of showing an “objective” reality. The purpose is instead to expose ideologies and their consequences in order to open them up to debate and allow people to attempt to influence and change them [55].

CDA can be done in different ways [18], and the aforementioned term “methodology” is probably a bad description for the approach because it can wrongly suggest that there is an algorithmic way of doing it. Here I undertake a type of CDA that is inspired by Habermas’ Theory of Communicative Action (TCA) [24]. Habermas is a suitable reference theoretician because he is part of the Frankfurt School tradition of critical theory. More importantly, his philosophy is strongly engaged in the “linguistic turn,” which means that he pays close attention to the role of language in philosophy and critical theory. It is not possible to do justice to Habermas’ complex theoretical framework here. (For good introductions cf. [34] or [30].

For Habermas communicative action is one of several action types. Communicative action is aimed at mutual understanding and collaboration. It has the moral characteristic of being based on the recognition of the other as a being with equal dignity. During communicative action, every utterance carries three so-called validity claims: truth (*Wahrheit*), (normative) rightness or legitimacy (*Richtigkeit*), and authenticity (*Wahrhaftigkeit*). That means that the speaker implies that the utterance is true, that it conforms to norms, and that he is sincere in saying it. All of these claims can be doubted by other participants in the communication. The

existence of disagreement regarding validity claims leads to discourses where the contentious claims can be contested through rational, fair, and open debate.

These basics of Habermas’ discourse theory can be used to develop a critical discourse analysis. I will follow Cukier *et al.* [14], [15] in basing my CDA on Habermas’ validity claims. The different validity claims are used to ask questions, which will allow the identification of instances of ideology in a text. Each validity claim leads to a variety of sub-questions, which are enumerated in Table I. The approach as developed by Cukier *et al.* is quite powerful because it allows a quantitative as well as qualitative analysis of texts. Here, I only use the approach as a heuristic to allow me to identify ideological claims.

### **Ideology of Privacy and Security – Some Evidence**

The main purpose of this article is conceptual. Its purpose is to argue that the moral and ethical nature of privacy and security can lead to their misuse as ideological tools. If I left it with this conceptual argument, however, there is a high probability that the paper would be accused of “arm-chair-philosophizing” i.e., of having no bearing on the “real world”. Critical research is not typically concerned about such criticism. On the other hand, some readers may find it easier to accept the argument if it provides some external validity or examples. The CDA described in this section therefore provides evidence of the link or links between ideology and privacy/security.

For this purpose, the CDA needed to investigate texts emanating from organizations that have an interest in security and privacy but at the same time have vested interests in promoting a particular ideological view. A first task was thus to consider which organization or organizations to investigate. The potential population included

all commercial entities involved in software or hardware. An obvious choice was therefore to look at Microsoft (MS), which as the biggest software company in the world has developed a broad range of activities in the areas of privacy and security. Microsoft is the market leader in operating systems and therefore its statements can be seen as representative of vendors to the end-user consumer market. Furthermore, Microsoft has often been criticized for its business practices and is seen as a bad example of market dominance and misuse by its detractors. It was therefore a reasonable starting point of the CDA to assume that Microsoft will use ideological devices to further its causes.

The next question was to decide which texts created by Microsoft to analyze. First, it was decided to use parts of the Microsoft website because they are easily accessible and, more importantly, because they represent the official views of the organization. Such statements are therefore more suitable to a discourse analysis than, say, interview data, which has a more idiosyncratic character. It then had to be decided which part of the website was to be analyzed. Two sections were chosen for detailed analysis: the “Trustworthy Computing” and the “Microsoft Vista” sites.

### **Validity Claims in Microsoft’s “Trustworthy Computing” and “Vista”**

Windows Vista ([www.microsoft.com/windowsvista](http://www.microsoft.com/windowsvista)) is the next generation of Microsoft’s operating system MS Windows, which was launched in late 2006. It is partly based on and closely linked with the considerations expressed in Microsoft’s “Trustworthy Computing” (TC) policy website (<http://www.microsoft.com/mscorp/twc/default.mspx>). Both websites outline the most important aspects of TC and Vista to promote acceptance of these developments by potential users. It is the nature of websites to be

dynamic and to contain links to other websites, so that limiting a discourse analysis to a website is necessarily a somewhat arbitrary endeavor. This is not overly problematic for the current research because its aim is to support the contention that moral concepts such as privacy and security can be used to promote ideology, rather than do a comprehensive analysis of a certain text or organization.

I analyzed the two websites with regards to the validity claims concerning privacy and security they contained. The TC site is structured in an overview page, which links to the five main components of TC, security, privacy, reliability, business practices, and building momentum. Each of these (except “building momentum”) is broken down in three sub-sections titled “overview”, “progress,” and “resources.”

The TC introductory page summarizes the aim of the TC initiative: “Trustworthy Computing is a long-term, collaborative effort to provide more secure, private, and reliable computing experiences for everyone. This is a core company tenet at Microsoft and guides virtually everything we do.” This summary indicates the different validity claims raised by the site. The central truth claim is that MS takes TC seriously and tries to promote and develop its components, including security and privacy. At the same time, it concedes that there “is no single solution to resolve computer security issues,” which is the reason for MS to explore all possible avenues to improve it.

In terms of rightness claims, there is no overt reference to ethics or morality but the website states clearly that it is in compliance with “global privacy laws.” Rightness also covers legitimacy, the assurance that one’s claims are acceptable. MS promotes this by portraying itself as a responsible leader, with the term “responsible leadership” being repeated in several different contexts. However, it is emphasized that MS does not act in isolation but col-

laborates closely with “industry, law enforcement, and academia”.

The sites authenticity/sincerity claims portray MS as a diligent organization, trying hard to help and support customers. The TC website states that MS is “hard at work every day,” that it “shares...knowledge [and] learn[s] from others,” and that it subscribes to the customers’ “right to control their personal information,” their right to be “left alone,” and their right to have a trusted experience. Since the authenticity claim can be explored by examining metaphors, the very concept of “trustworthy computing” can be interpreted as a metaphor aimed at promoting the image of sincerity.

The Vista website is structured in a similar way to the TC site but it is more clearly directed at end-users and has a less formal and informational appearance. It is divided into three main areas: experience, features, and community. It contains a variety of claims regarding privacy and security, which are probably best summarized by the following quote: “At Microsoft, we recognize that privacy is a critical element of a secure computing experience.” Privacy is thus subsumed into security, which is recognized as a central aspect of Windows. Vista is meant to be “the most secure version of Windows yet.” There are many instances where the document underlines the centrality of security for Vista from the perspective of private users, businesses, and developers. Security features are integrated into the software and can be controlled and managed centrally.

The normative claims mirror the emphasis on security. They underline how increased security will render the tasks of systems administrators easier while allowing end users to engage in (apparently legitimate) activities such as enjoying TV and music on their PC. Probably the strongest claim to legitimacy is linked to the protection of children. A centralized control function allows children to be protected from innocently

installing malware. Another function (“family safety settings”) allows parents to designate what children can do on the computer, including access to programs, websites, and keeping a log of all activity.

The authenticity/sincerity claims support the implication that MS is serious about helping its customers. The website uses emotive images, such as a lonely figure on a mountaintop in the twilight to express feelings of independence and strength. The “features” part of the website starts by displaying a young tattooed man of presumably African background holding a guitar, which expresses a connection to younger consumers and their wish for freedom. Another interesting sincerity claim is the metaphor of the word “vista” itself. According to the Oxford English Dictionary, vista can mean “A mental view or vision of a far-reaching nature.” This can be interpreted to imply that MS has recognized customers’ needs (particularly security) and has integrated them into its long-range vision.

### **Ideology in Microsoft’s “Trustworthy Computing” and “Vista”**

The discussion of the validity claims contained in MS’s two websites under investigation will probably not surprise anyone. They project the image of a corporation interested in its customers’ well-being and therefore sensitive to their moral concerns, including security and privacy. The interesting question therefore is whether there is evidence of instances of ideology and what the consequences of the promotion of such ideology might be.

One such instance is the use of rhetorical devices to cloak underlying problems. An example of this is the use of the term “trustworthy computing,” which MS adopted recently having changed it from “trusted computing” [1]. It is probably fair to say that MS is not trusted by a considerable part of the computer science and programming commu-

nity. Trust is a complex social construct but it is not something that can simply be created. There clearly seems to be a lack of trust in computing by users, largely due to a perceived lack of security and privacy [12]. Microsoft uses a rather technical view of trust [1] but does not elaborate on this concept in its websites. The emphasis on trustworthy computing is therefore misleading because it is an open question whether Microsoft's and their customers' understanding of trust are compatible.

A similar issue arises with regard to the functionality of Vista. The website frequently cites issues of control and implies that it will give control to users ("Windows Vista puts you in control of what you want to do"). It is meant to create confidence in customers and improve their "computing experience." These are very problematic assertions as I will show below.

Both websites privilege particular interests, most notably those of Microsoft and its paying customers. This goes counter to the nature of security problems, which are collective issues and cannot be solved by individual or sectoral activities. Among customers, corporate interests are again privileged. Despite some of the emancipatory rhetoric, the website makes it clear that, internally, MS relies on hierarchical power structures to enforce its policies, including privacy policies. The validity claims raised on the website also use one of the most powerful instruments of ideology, that of reification. Most importantly, it reifies both security and privacy.

In practice this means that these two concepts become things, which are still morally relevant, but no longer open to debate and scrutiny. The way this is done is to present privacy and security as technical features, which can be addressed in a technical way. The best example of this reification of a social construct is that MS aims to "engineer privacy into our products during the

product life cycle." It thus becomes a matter of technical expertise, which MS has without doubt, to deal with this issue. This reification also allows a simplification of the complex relationship of privacy and security by subsuming privacy as an aspect of security.

This leads us to another ideological device, the hiding of contentious relationships. The equation or subsumption of privacy under security hides the fact that there is no simple law stating that more privacy will create more security or vice versa. In the "privacy progress" part of the TC site, MS states that it is committed to working with the police to deter hacking and other "software sabotage" through proactive security practices. It ignores the fact that there may be good reasons for hacking. The law-enforcement attitude leaves no room for legitimate expressions such as "hacktivism".

By complying with laws on security and privacy without ethical reflection, MS promotes a one-sided understanding of complex issues. This has recently backfired when Microsoft was criticized for complying with the Chinese government's request to curtail free speech on the Internet. The unidimensional narrative on the website, while serving corporate purposes leaves no opening for dissenting voices and hides legitimate conflicts. It also camouflages the fact that many of the problems current developments are supposed to address, such as lack of security, are home-grown problems that have been caused by Microsoft's long-time lack of attention.

Another instance where the claims on the website hide an important moral issue has to do with control. MS Vista offers an unprecedented amount of control over user activities. This is described in positive terms as ease of administration and supervision of children. It is quite obvious, however, that the same technologies can be used to control and surveil employees.

There is a large body of literature on the moral issues of workplace surveillance [71], but the reification of privacy hides these. Another completely hidden issue is the question of digital rights management (DRM). DRM raises a host of moral and legal challenges and is likely to be linked to MS Vista. The website does not discuss any of these issues, presumably because of the simplistic approach that MS will comply with the laws (which it often shapes) and thereby discharge its moral responsibilities.

### Critical Reflections

I have argued that privacy and security are concepts with important moral connotations. I then suggest that these moral qualities render the concepts open to be used to promote certain ideologies. Finally, I have attempted a brief critical discourse analysis on Habermas' Theory of Communicative Action to support the suspicion that the moral nature of privacy and security can be used for ideological purposes.

This work does not suggest that ideology can be overcome once and for all. Ideology is part of the pre-judgments that we require to function as social beings. It does suggest, however, that ideologies can be exposed and thereby put into perspective. Furthermore, this work should not be misread as another example of Microsoft-bashing. Microsoft's websites were used because of the overwhelming market power of the corporation and because it exemplifies the issues raised here. A similar exercise could most probably be undertaken for the majority of ICT suppliers.

Another point of criticism might be that this paper does nothing more than state the obvious. Microsoft is a commercial entity and as such attempts to promote itself and its causes. While this is true, the interesting aspect of the preceding discussion is that it demonstrates how official publications of corporations use and thereby reproduce ideologi-

cal views. A statement to the effect that we should not believe promotional commercial publications would only show that communicative action seems to be impossible in our society, which, if true, should give us pause to consider whether this is what we as a society desire.

Most of all, I hope this article will promote debate on the relationship between ethics, technology, and ideology. The unique angle elaborated here is that it is exactly the moral connotation of notions such as privacy and security that allows them to be used to defend ideology. It is the moral recognition of privacy and the protection of children that allows Microsoft to promote a strict system of control, which, if exposed as such, would be much more difficult to market. Similarly, security has now become such an obviously desirable goal that it can be used to override other legitimate democratic and moral concerns.

This article, by its very nature, does not offer any solutions to these problems. It can only aim to raise attention and awareness and to promote discourse. In the tradition of critical research, its main aim is to provide a dissenting voice and to caution users not to take concepts at face value. This is particularly important for value-laden concepts because these values, positive as they may be, hold the potential to curtail debate and thereby allow for the promotion of ideology. In this sense, the paper should have an emancipatory effect. It will allow individuals to question the meaning of privacy and security and to require contextualization of the terms. This can help free us from false preconceptions and thus allow us to move, albeit incrementally, toward more freedom and autonomy.

### Author Information

The author is with the Faculty of Computer Science and Engineering, Centre for Computing and Social Responsibility, De Montfort Uni-

versity, The Gateway, Leicester LE1 9BH, U.K.; bstahl@dmu.ac.uk.

### References

- [1] R. Anderson, "Cryptography and competition policy - Issues with 'trusted computing'," in *Economics of Information Security*, L.J. Camp and S. Lewis, Eds. Dordrecht, Germany: Kluwer, 2004, pp. 35-52.
- [2] R.E. Anderson, D.G. Johnson, D. Gotterbarn, and J. Perrolle, "Using the new ACM Code of Ethics in decision making," *Commun. ACM*, vol. 36, no. 2, pp. 98-106, 1993.
- [3] M. Alvesson and S. Deetz, *Doing Critical Management Research*. London, U.K.: SAGE, 2000.
- [4] B. Berendt, O. Gunther, and S. Spiekerman, "Privacy in e-commerce: Stated preferences vs. actual behavior," in *Commun. ACM.*, vol. 48, no. 4, pp. 101-106, 2005.
- [5] J.J. Britz "Ethical guidelines for meeting the challenges of the information age," in *Ethics and Electronic Information in the 21st Century*, L.J. Pourciau, Ed. West Lafayette, IN: Purdue Univ. Press, 1999, pp. 9-28.
- [6] C. Brooke, "What does it mean to be 'critical' in IS research?," *J. Information Technology*, vol. 17, pp. 49-57, 2002.
- [7] W.S. Brown, "Ontological security, existential anxiety and workplace privacy," *J. Business Ethics*, vol. 23, pp. 61-65, 2000.
- [8] L.J. Camp, "Web security and privacy: An American perspective," in *Readings in Cyberethics*, R.A. Spinello and H.T. Tavani, Eds. Sudbury, MA.: Jones and Bartlett, 2001, pp. 474-486.
- [9] L.J. Camp and S. Lewis, Eds. *Economics of Information Security*. Dordrecht, Germany: Kluwer, 2004.
- [10] L.J. Camp and C. Wolfram, "Pricing security - A market in vulnerabilities," in *Economics of Information Security*, L.J. Camp and S. Lewis, Eds. Dordrecht, Germany: Kluwer, pp. 17-34, 2004.
- [11] S. Chan and L.J. Camp, "Law enforcement surveillance in the network society," *IEEE Technology and Society Mag.*, vol. 21, no. 2, pp. 22-30, 2002.
- [12] H. Cavusoglu, "Economics of IT security management," in *Economics of Information Security*, L.J. Camp and S. Lewis, Eds., Dordrecht, Germany: Kluwer, pp. 71-83, 2004.
- [13] M.J. Culnan, "How did they get my name?: An exploratory investigation of consumer attitudes toward secondary information use," *MIS Quarterly*, vol. 17, no. 3, pp. 341-363, 1993.
- [14] W. Cukier, C. Middleton, and R. Bauer, "The discourse of learning technology in Canada: Understanding communication distortions and the implications for decision making," in *Global and Organizational Discourse About Information Technology*, E. Wynn, E. Whitley, M. Myers, and J. DeGross, Eds. Dordrecht, Germany: Kluwer, 2003, pp. 197-221.
- [15] W. Cukier, C. Middleton, and R. Bauer, "Applying Habermas' validity claims as a standard for critical discourse analysis," in *Information Systems Research - Relevant Theory and Informed Practice*, B. Kaplan, D. Truex, T. Wood-Harper, and J. DeGross, Eds. Dordrecht, Germany: Kluwer, 2004, pp. 233-258.
- [16] D. Elgesiem, "Privacy, respect for persons, and risk," in *Philosophical Perspectives on Computer-Mediated Communication*, C.

Ess, Ed. Albany NY.: State Univ. of New York Press, 1996, pp. 45-66.

- [17] N. Fairclough, *Analysing Discourse - Textual Analysis for Social Research*. London, U.K., and New York, NY: Routledge, 2003.
- [18] N. Fairclough, *Critical Discourse Analysis - The Critical Study of Language*. London, U.K.: Longman, 1995.
- [19] A. Feenberg, *Questioning Technology*. London, U.K.: Routledge, 1999.
- [20] T. Forester and P. Morrison, *Computer Ethics - Cautionary Tales and Ethical Dilemmas in Computing*, 2nd ed. Cambridge, MA/London, U.K.: M.I.T. Press, 1994.
- [21] D. Gauthier, *Morals by Agreement*. Oxford, U.K.: Clarendon, 1986.
- [22] R. Gavison, "Privacy and limits of law," in *Computers, Ethics and Social Values*, D.G. Johnson and H. Nissenbaum, Eds. Upper Saddle River, NJ: Prentice Hall, pp. 332-351, 1995.
- [23] A. Giddens, *The Constitution of Society - Outline of the Theory of Structuration*. Cambridge, U.K.: Polity, 1984.
- [24] J. Habermas, *Theorie des kommunikativen Handelns - Band I/II*, Frankfurt, Germany: Suhrkamp Verlag, 1981.
- [25] J. Habermas, *Technik und Wissenschaft als 'Ideologie'*. Frankfurt, Germany: Suhrkamp, 1969.
- [26] R. Hirschheim, H.K. Klein and K. Lyytinen, *Information Systems Developing and Data Modeling: Conceptual and Philosophical Foundations*. Cambridge, U.K.: Cambridge Univ. Press, 1995.
- [27] R. Hirschheim and H.K. Klein, "Realizing emancipatory principles in information systems development: The case for ETHICS," *MIS Quarterly*, vol. 18, no. 1, pp. 83-109, 1994.
- [28] D.L. Hoffman, T.P. Novak, and M. Peralta, "Building consumer trust online," *Commun. ACM*, vol. 42, no. 4, pp. 80-87, 1999.
- [29] L. Inrona, "Privacy and the computer - Why we need privacy in the information society," in *Cyberethics - Social and Moral Issues in the Computer Age*, R.M. Baird, R. Ramsower, and S.E. Rosenbaum, Eds. New York, NY: Prometheus, 2000, pp. 188-199.
- [30] M. Janson and D. Cecez-Kecmanovic, "Making sense of e-commerce as social action," *Information Technology and People*, vol. 18, no. 4, pp. 311-342, 2005.
- [31] D.G. Johnson, *Computer Ethics*, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2001.
- [32] R. Khare and A. Rifkin "Trust management on the World Wide Web," *First Monday*, vol. 3, no. 6, 1998; www.firstmonday.dk.
- [33] M. Klang "A critical look at the regulation of computer viruses," *Int. J. Law and Information Technology*, vol. 11, pp. 162-183, 2003.
- [34] H.K. Klein and M.Q. Huynh "The critical social theory of Jürgen Habermas and its implications for IS research," in *Social Theory and Philosophy for Information Systems*, J. Mingers and L. Willcocks, Eds. Chichester, U.K.: Wiley, 2004, pp. 157-237.
- [35] C.E. Landwehr, *A Survey of Formal Models for Computer Security*, NRL Rep. 8489. Washington D.C.: Naval Research Laboratory, 1981.
- [36] C.E. Landwehr, C.L. Heitmeyer, and J.D. McLean, "A security model for military message systems: Retrospective," Naval Research Laboratory, Washington, DC, 2001; <http://chacs.nrl.navy.mil/publications/CHACS/2001/2001landwehr-ACSAC.pdf>, accessed Apr. 1, 2006.

- [37] D. Lyon, *Surveillance after September 11*. Cambridge, U.K.: Polity, 2003.
- [38] R.O. Mason, "Four ethical issues of the information age," *MIS Quarterly*, vol. 10, pp. 5-12, 1986.
- [39] L. McAulay, N. Doherty, and N. Keval, "The stakeholder dimension in information systems evaluation," *J. Information Technol.*, vol. 17, pp. 241-255, 2002.
- [40] J.H. Moor, "Reason, relativity, and responsibility in computer ethics," in *Computer Ethics and Professional Responsibility*, T.W. Bynum and S. Rogerson, Eds. Oxford, U.K.: Blackwell, 2004, pp. 21-38.
- [41] J.H. Moor, "If Aristotle were a computing professional," in *Cyberethics — Social and Moral Issues in the Computer Age*, R.M. Baird, R. Ramsower, and S.E. Rosenbaum, Eds. New York, NY: Prometheus, 2000, pp. 34-40.
- [42] J.H. Moor, "Toward a theory of privacy in the information age," in *Cyberethics — Social and Moral Issues in the Computer Age*, R.M. Baird, R. Ramsower, and S.E. Rosenbaum, Eds. New York, NY: Prometheus, 2000, pp. 200-212.
- [43] J.H. Moor, "What is computer ethics?," *Metaphilosophy*, vol. 16, no. 4, pp. 266-275, 1985.
- [44] P. Nikander and K. Karvonen, "Users and trust in cyberspace," *Cambridge Security Protocol Workshop*, 2000.
- [45] H. Nissenbaum, "Where computer security meets National security," *Ethics and Information Technology*, vol. 7, no. 2, pp. 61-73, 2005.
- [46] H. Nissenbaum, "Can trust be secured online? A theoretical perspective," *etica and politica*, vol. 1, no. 2, 1999; <http://www.units.it/~etica/>, accessed May 26, 2006.
- [47] W.J. Orlikowski and J.J. Baroudi, "Studying information technology in organizations: Research approaches and assumptions," *Information Systems Research*, vol. 2, no. 1, pp. 1-28, 1991.
- [48] N. Postman, *Technopoly - The Surrender of Culture to Technology*. New York, NY: Vintage, 1992.
- [49] J. Rachels, "Why privacy is important," in *Computers, Ethics and Social Values*, J.G. Johnson and H. Nissenbaum, Eds. Upper Saddle River, NJ: Prentice Hall, 1995, pp. 351-357.
- [50] W.L. Robison, "Privacy and appropriation of identity," in *Ethics in the Age of Information Technology*, G. Collste, Ed. Linköping, Sweden: Centre for Applied Ethics, 2000, pp. 70-86.
- [51] S. Rogerson, *Ethical Aspects of Information Technology - Issues for Senior Executives*. London, U.K.: Institute of Business Ethics, 1998.
- [52] M. Rotenberg, "Communications Privacy: Implications for Network Design," in *Ethics, Information and Technology: Readings*, R. Stichler and R. Hauptman, Eds. Jefferson, NC: MacFarland, 1998, pp. 152-168.
- [53] J. Rutter, "From the sociology of trust towards a sociology of 'e-trust,'" *Int. J. New Product Development and Innovation Management*, vol. 2, no. 4, pp. 371-385, 1999.
- [54] S. Sahay, "Beyond utopian and nostalgic views of information technology and education: Implications for research and practice," *J. Association for Information Systems*, vol. 5, no. 7, pp. 282-313, 2004.
- [55] K. Saravanamuthu, "Information technology and ideology," *J. Information Technology*, vol. 17, pp. 79-87, 2002.
- [56] J. Schumpeter, "Science and ideology," in *The Philosophy of Economics: An Anthology*, 2<sup>nd</sup> ed., D.M. Hausman, Ed. Cambridge, U.K.: Cambridge Univ. Press, 1994, pp. 224-238.
- [57] R.J. Severson, *The Principles of Information Ethics*. Armonk, NY/London, U.K.: M. E. Sharpe, 1997.
- [58] A. Shostack and P. Syverson, "What price privacy? (and why identity theft is about neither identity nor theft)," in *Economics of Information Security*, L.J. Camp and S. Lewis, Eds. Dordrecht, Germany: Kluwer, pp. 129-142, 2004.
- [59] J.C. Sipiior and B.T. Ward, "The ethical and legal quandary of email privacy" *Commun. ACM*, vol. 38, no. 12, pp. 48-54, 1995.
- [60] R. Spinello, *Case Studies in Information and Computer Ethics*. Upper Saddle River, NJ: Prentice Hall, 1997.
- [61] B.S. Stahl, M. Prior, S. Wilford, and D. Collins, "Electronic monitoring in the workplace: If people don't care, then what is the relevance?," in *Electronic Monitoring in the Workplace: Controversies and Solutions*, J. Weckert, Ed. Hershey, PA: Idea-Group, 2005, pp. 50-78, 2005.
- [62] B.C. Stahl, "Responsibility for information assurance and privacy: A problem of individual ethics?," *J. Organizational and End User Computing* (Special Issue on Information Assurance and Security), C.D. Schou and K.J. Trimmer, Eds., vol. 16, no. 3, pp. 59-77, 2004.
- [63] B.C. Stahl, *Responsible Management of Information Systems*. Hershey, PA: Idea Group, 2004.
- [64] D.W. Straub and R.W. Collins, "Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy," *MIS Quarterly*, vol. 14, pp. 143-156, 1990.
- [65] H. Tavani, "Privacy and security," in *Internet Ethics*, D Langford, Ed. London, U.K.: McMillan, 2000, pp. 65-89.
- [66] H.T. Tavani and J.T. Moor, "Privacy protection, control of information, and privacy-enhancing technologies," in *Readings in Cyberethics*, R.A. Spinello and H.T. Tavani, Eds. Sudbury, MA: Jones and Bartlett, 2001, pp. 378-391.
- [67] M. Velasquez, *Business Ethics: Concepts and Cases*, 4th ed. Upper Saddle River, NJ: Prentice Hall, 1998.
- [68] J. Viega, T. Kohno and B. Potter, "Trust (and mistrust) in secure applications," *Commun. ACM*, vol. 44, no. 2, pp. 31-36, 2001.
- [69] C. Wall and J. Paroff, "Cracking the computer forensics mystery," *Computer and Internet Lawyer*, vol. 22, no. 4, pp. 1- 6, 2005.
- [70] S.D. Warren and L.D. Brandeis, "The right to privacy" *Harvard Law Rev.*, vol. 5, pp. 193-220, 1890.
- [71] J. Weckert, Ed. *Electronic Monitoring in the Workplace: Controversies and Solutions*. Hershey, PA: Idea-Group, 2005.
- [72] J. Weckert and D. Adeney, *Computer and Information Ethics*. Westport, CT/London, U.K.: Greenwood, 1997.

## IEEE-SSIT Distinguished Service Award

The IEEE-SSIT Distinguished Service Award was approved by the IEEE Board of Directors in November 2006. The award will be given annually to a full member of SSIT who has served the society in an exemplary way for a period of years. Service may be as a board member, contributor to publications, conference organizer, or any combination of these or other activities. Candidates will be judged on length, breadth, and impact of service.

The award will consist of a plaque, given at SSIT's annual conference, the International Symposium on Technology and Society (ISTAS).

SSIT's Awards Committee seeks nominations for this award for 2007. Nominations are due March 31, 2007, with selection and approval completed by April 30, and notification of the recipient by May 15.

Please send nominations or requests for information to Janet Rochester at [j.rochester@ieee.org](mailto:j.rochester@ieee.org).