How to Do Computer Ethics—A Case Study: The Electronic Mall Bodensee

Terrell Ward Bynum
Southern Connecticut State University, USA

Petra Schubert
University of St. Gallen
Switzerland

Abstract: *In this article the authors present a model of ethical analysis and decision making for the field of computer ethics--a model that actually works for all areas of applied ethics. It is argued that a rich and complex fabric of "policies for conduct"--a "received policy cluster (RPC)--is used by computer ethics decision makers in a dynamic process similar to Rawls's "wide reflective equilibrium" (WRE). This "policy-cluster model" makes use of Moor's classic definition of the field of computer ethics and van den Hoven's suggested use of Rawlsian WRE. To indicate how the policy-cluster model can be applied, we present and analyze some privacy and security issues regarding the Electronic Mall Bodensee, which is a World-Wide-Web-based business project in Central Europe.*

1 Introduction

In the mid 1970s, when Maner first coined the term "computer ethics" [see Maner, 1980], medical ethics was the most mature field of applied ethics. For this reason, medical ethics often served as a model for other areas like business ethics or journalism ethics. According to the medical ethics model at that time, the way to do applied ethics was to apply philosophical theories like utilitarianism and Kantianism to specific cases and dilemmas. Standard textbooks in applied ethics typically contained an early chapter in which utilitarian and Kantian ethical theories were spelled out or summarized. In the early days of computer ethics (1970s), Maner recommended a similar methodology.

Even though many textbooks and other writings in applied ethics in the 1970s and 1980s paid lip service to this "medical ethics" model of doing applied ethics, a glance through the pages of these books reveals that the model was rarely actually followed--even in medical ethics itself. In most applied ethics textbooks of that time, one finds chapter after chapter with little or no Kantian or utilitarian analyses. The newly emerging field of computer ethics was no exception. For example, one of the first--and certainly most influential--textbooks in the field was Johnson's *Computer Ethics* (1985). The first chapter of this book was devoted primarily to utilitarian and Kantian theory, but the vast majority of the ethical analyses in the rest of the book ignore those theories.

During the past decade, applied ethics--including computer ethics--has become methodologically more sophisticated. For example, additional philosophical theories such as Aristotelian virtue theory and social contract theory have been added to the list of suggested philosophical tools. [See, for example, Edgar, 1997, and Spinello, 1995, 1997]. But more importantly, instead of remaining in the very abstract realm

of broad philosophical principles like Kant's "categorical imperative" or Bentham's "principle of utility", applied ethicists have begun to pay more attention to a wide diversity of less abstract guides to conduct such as laws, professional codes and accepted standards of practice.

At the same time, computer ethics scholars have been developing a variety of "how-to-do-it" *models* for performing ethical analyses and reaching ethical conclusions. [Collins and Miller, 1992], for example, offer a four-step "paramedic method"; and [Langford, 1995] even provides a seventeen-component "flow chart". Perhaps the richest and most complex model of computer ethics decision making so far is that of [Spinello,1995, 1997], whose seven-step procedure involves consideration of laws, moral intuitions, corporate and professional codes of ethics, philosophical theories and public-policy implications.

In the present essay, we offer yet another model of ethical analysis and decision-making for computer ethics (and indeed for *any* kind of applied ethics). We believe that this model comes closer than previous ones to capturing *what actually happens* when practicing computer professionals (and people in general) make ethical judgments and choices. [See Bynum, 1997, Chapter 2] To develop this new model, we make use of Moor's classical definition of the field of computer ethics in his article "What Is Computer Ethics?" (1985), and also of a Rawlsian approach to decision-making sketched out by van den Hoven in his article "Computer Ethics and Moral Methodology" (1996). The model expands upon Spinello's insight (1995, 1997) regarding the richness and diversity of the guides to conduct that ethical decision makers actually use in real-life situations.

2 Identifying Policy Vacuums

During the past decade, Moor's definition of computer ethics in his article "What Is Computer Ethics?" has been the most influential one. It is a broad definition that is independent of any specific philosopher's ethical theory. In addition it is compatible with a variety of approaches to ethical problem-solving. Moor defines computer ethics as a field concerned with "policy vacuums" and "conceptual muddles" regarding the social and ethical use of information technology:

> A typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used. Computers provide us with new capabilities and these in turn give us new choices for action. Often, either no policies for conduct in these situations exist or existing policies seem inadequate. A central task of computer ethics is to determine what we should do in such cases, that is, formulate policies to guide our actions.... One difficulty is that along with a policy vacuum there is often a conceptual vacuum. Although a problem in computer ethics may seem clear initially, a little reflection reveals a conceptual muddle. What is needed in such cases is an analysis that provides a coherent conceptual framework within which to formulate a policy for action. (p. 266)

Moor says that computer technology is genuinely revolutionary because it is "logically malleable":

> Computers are logically malleable in that they can be shaped and molded to do any activity that can be characterized in terms of inputs, outputs and connecting logical operations....Because logic applies everywhere, the potential applications of computer technology appear limitless. The computer is the nearest thing we have to a universal tool. Indeed, the limits of computers are largely the limits of our own creativity. (p.269)

On Moor's view, then, computer technology is powerful and revolutionary because it is logically malleable. It creates opportunities to do new things that we could never do before. The question then becomes whether we *should* do these things. To answer this ethical question, we need to determine whether already existing "policies for conduct" cover the new things that we can do. If the answer is "yes", then normally we should simply follow the existing policies. But what "policies for conduct" should we look at?

The old 1970s "medical ethics" model of applied ethics would recommend that we look to abstract principles of the philosophers, such as the "principle of utility" of Bentham, "the categorical imperative" of Kant, the "virtues and vices" of Aristotle, and so on. We believe, however, that a typical ethical decision maker--including a typical computer professional--looks to much less grandiose "policies for conduct". The usual ethical decision maker uses personal values and standards derived from the family and the community. And if the decision-maker is an employed professional who belongs to a professional organization, he or she may well apply accepted "standards of good practice" of the profession, or corporate codes of ethics, or codes of ethics of professional organizations like the Association for Computing Machinery or the British Computer Society. At the same time, of course, a cluster of national, state and local laws may apply; and in these days of world-wide computing and commerce, there are likely to be international agreements and laws as well.

There exists, therefore, for each person or group making ethical decisions, a complex set of received "policies for conduct" (henceforth the RPC). This set of behavioral rules and guides for ethical conduct forms a multi-leveled, rich-textured fabric of overlapping rules, principles, laws and practices to inform one's ethical judgments and actions. Most of the time, an ethical decision maker with good judgment will be able to apply his or her RPC to a particular case, see how the case fits the rules, and then make the appropriate ethical decision.

But if computer technology is so revolutionary that it generates *new* kinds of cases which do not easily match the RPC, how should one proceed? Our decision-maker now faces one of Moor's "policy vacuums". It is at this point that the abstract, carefully-reasoned moral theories of the philosophers may prove to be useful. And it is also at this point that the Rawslian notion of "wide reflective equilibrium" (WRE) can provide insight into the dynamic process of adjusting or adding policies to cope with novel cases.

3 Wide Reflective Equilibrium with the RPC

Faced with a Moorian policy vacuum, our decision maker must make a "considered moral judgment", using the received policy cluster of his or her community and society. If, in addition, he or she also knows the powerful ethical theories developed by philosophers (utilitarianism, Kantianism, virtue theory, social contract theory, etc.), then these too can be added to the decision maker's "tool kit" for ethical thinking.

We agree with van den Hoven (1996) that the appropriate decision process here can be viewed as the kind of dynamic interaction which Rawls (1971) called "wide reflective equilibrium" (WRE), and which is described by Griffin this way:

> The best procedure for ethics . . . is going back and forth between intuitions about fairly specific situations on the one side and the fairly general principles that we formulate to make sense of our moral practice on the other, adjusting either, until eventually we bring them all into coherence. [Griffin, 1993]

In our view--adopting a Rawlsian approach--the appropriate way to understand ethical decision making in computer ethics (or indeed in any other area of applied ethics) is as a complex interaction of three elements: (1) the considered moral judgments of the decision maker(s); (2) policies for conduct--in our case, we take these to be the rich and complex RPC plus the abstract ethical theories of the philosophers; and (3) background theories about the world and how it works. Van den Hoven describes that process this way:

> The general procedure involved in achieving a mutual fit is that of shuttling back and forth between considered moral judgments about a case and our moral principles, adjusting each in light of the other and in light of the relevant background theories, in order to arrive at reflective equilibrium. This state is called 'reflective' because we know to what principles our judgments conform, and it is referred to as an 'equilibrium' because principles and judgments coincide. (p. 449)

Summary of the "Policy Cluster Model"

Given Moor's account of the nature of computer ethics, our "policy-cluster model" for doing computer ethics can be summarized as follows. When information technology suddenly makes it possible to do something that could not be done before, one must decide whether it would be ethical to actually *do* it, or whether it would be right to *allow* others to do it. To help answer this and related ethical questions, every decision maker--whether it be a person, a group of persons, an organization of some sort, or even a nation--has a complex web of overlapping, interweaving "policies for conduct", which we have called the "received policy cluster" (RPC). This powerful and complex guide to conduct has many different levels and layers:

> International Treaties and Agreements -- The widest level of policies to govern conduct, at least in the geographic sense, is the complicated set of international treaties and agreements, including international law, global business agreements and conventions, government to government treaties, and so on. Computing related agreements include, for example, policies on ownership of intellectual property, security, encryption of data, and so on.
>
> Laws -- Nations, provinces, cities and local governments, of course, all have thousands of laws, many of which apply to computer-related conduct from public disclosure of databases to privacy of information, from laws against hacking and computer viruses to statutes governing ownership of software.
>
> Regulations -- In addition to laws themselves, there are thousands of government regulations laid down by various agencies and departments to interpret and carry out the laws.
>
> Professional Codes of Conduct -- On top of treaties, laws and government regulations, there are codes of conduct adopted by professional organizations. Such codes may apply, for example, to computer professionals who are members of groups like the Association for Computing Machinery (ACM), the British Computer Society (BCS), and so on.

Corporate Policies -- In addition to treaties, laws, government regulations and professional codes, large corporations often add their own rules of conduct for their employees. Such policies can include, for example, rules for the use of company computers, standards for software testing and quality assurance, and so on.

Standards of Good Practice -- Entire professional communities sometimes reach agreement on "standards of good practice" that every practitioner in that field is expected to uphold. In computing, for example, there are standards of good practice for software engineering and data encryption.

Community and Personal Standards -- In addition to *formal* rules and regulations like those listed above, a decision maker typically functions within a setting that has a wide diversity of *unwritten* "common practices" and morés. These often depend upon a specific country, community or family to which a professional belongs. Indeed, individuals usually include their own *personal standards of conduct* in the fabric of policies that influence their decisions and judgments.

Given the richness and complexity of this "received policy cluster", Moorian policy vacuums can occur at many different levels. Thus for example creation of the Internet, especially the World-Wide-Web part of it, has made it possible--for the first time in history--for children all over the world to easily access hard-core pornography in their own homes. Is this ethically acceptable? Should there be family policies that individual parents create? Should Internet access companies create corporate policies to deal with the question of hard-core pornography and children? Should libraries and schools have policies? Should local, state and national governments pass laws? Should there be international agreements and treaties? These and many other questions require attention at many different levels of responsibility; and the RPC is the starting point for creating new policies to fill the gaps.

4 The Case of the Electronic Mall Bodensee

As an example of how our proposed model of ethical decision making works, we present here an analysis of a specific case: the Electronic Mall Bodensee and how it is dealing with privacy and security issues.

The Electronic Mall Bodensee (emb.net) project was launched in January 1995 to develop and implement a regional, electronic marketplace in the area around Lake Constance in Europe. One major goal of the EMB was to strengthen the economy of the region, utilizing the potential of new telematic infrastructures of the information age. It is based on Internet technology. Although multinational in nature, the EMB creates an open electronic marketplace for a specific region--the Lake Constance region-- which covers parts of Austria, Germany and Switzerland in the heart of Europe.

The EMB serves as an example for observation of business transactions between different partners on a regional scale. Two-years of experience in electronic commerce have highlighted a number of important issues, especially the currently prevailing problem of *acceptance*, which is still a significant hurdle for electronic market platforms. Thus, even though the EMB offers a number of technically mature shopping possibilities, there has not been a real breakthrough of electronic shopping during the last two years. And although the EMB, in principle, enables world-wide access, business has been rather regionally limited. This is due, in

part, to the fact that some shops offer their products only in German. Another big obstacle is currency. When it comes to payment, vendors accept only their local currency--in this case Austrian Shillings or German Marks or Swiss Francs. Because of this, settlement becomes very expensive for the buyer because banks charge high transfer and exchange fees. The introduction of the Euro (the expected future European currency) will help to overcome some of these problems, at least as far as the Bodensee region is concerned. Trading on a global scale, however, will still have to await the implementation of a user-friendly, trustworthy system for payment settlement.

Besides language and payment problems, logistics play an important part in business on the Internet. For example, the net serves as an ideal channel for distribution of digital goods; but vendors of tangible goods face the same problems as a mail-order business (transportation, insurance, import/export regulations, postal fees, and so on). An instructive example is provided by a regional vendor of wine-- an example supporting the hypothesis that customers still seek personal contact as well as real-life shopping experiences. Many clients of a wine shop in St. Gallen reported that surfing in the Electronic Mall Bodensee called their attention to the shop, but instead of ordering via the Internet they decided to personally visit the shop.

4.1 Privacy and Electronic Shopping

Traditionally, the term “privacy” has meant at least two different (but related) things:

1. The right to close the door behind us and thus be left alone.
2. The freedom to determine with whom we share personal details of our lives or personal information. [Tapscott, 1996]

The question of privacy is as old as mankind, but with the increasing operation of computers and computer networks it has become an urgent issue. As electronic commerce evolves, information about a person’s shopping behavior becomes more and more valuable and, at the same time, easier to acquire. Large databases facilitate access to information and it is becoming easier to trace activities in electronic media. Formerly, it was feasible to track the activities of one or two people (accessing paper files usually meant phoning and traveling a lot), but it would have been impossible to track thousands of people on a routine basis. The possibility of automation--of mighty electronic “robots” which comb the Internet for consumer habits or credit card information--really makes privacy an issue.

One possibility of protecting ourselves against loss of privacy is *not to participate* in the Electronic World. This approach corresponds to closing the door behind ourselves. But what if there are big opportunities--special bargains, exiting new products--on the Web which we do not want to miss? What is the information that we believe is too private to be handed over to a merchant? When it comes to a business transaction it is usually not possible for the customer to stay anonymous. Some personal information must be revealed. In the case of a physical product, for example, (there are different criteria for electronic products, which can be delivered directly via the Internet):

- Choice of product
- Dispatch address
- Number and time of shopping visits
- Amount spent
- Payment information (e.g. credit card number and validation date)

It is obvious that this information can be used to draw up specific customer profiles. The product information can be collected and grouped into special product segments. A customer who buys all CDs of Elton John, for example, is most likely to be interested in new ones. Clever marketers can derive all sorts of preferences from such a profile, thus possibly stimulating customers to buy things they do not really need.

Of course, revealing information about shopping habits is only one side of the coin. Payment information is even riskier for mischievous or fraudulent activities. So it is important to protect payment data from unauthorized persons.

Electronic market platforms are able to solve part of these problems. To understand the role they play in Electronic Commerce, we have first to take a look at customer-vendor relationships in electronic environments. There are two possible business scenarios for an electronic shopping relationship.

4.2 Scenario One: Direct Customer-Merchant Relationship

There are two different security risks within this scenario:

1. Transfer of data via the Internet
2. Local storage (on the merchant's computer).

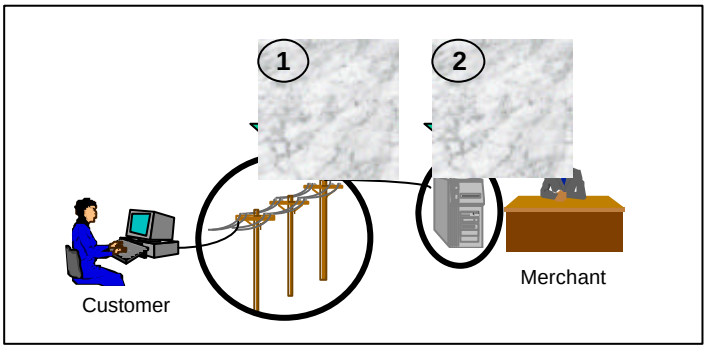

Figure 1: Two stages of privacy flaws

Let us consider these in order.

Transfer of information--The first security risk is clearly the most discussed in recent literature. Due to the open nature of the Internet, one can never know with certainty which path information from a given Point A (customer) to a second Point B (merchant) will take. Along the way, there are plenty of possible eaves-

droppers who can copy the data and use it for unethical activities. As indicated in the following section, there are several encryption techniques available to scramble data and make it useless for potential "sniffers".

Information Storage--The second risk is less talked about, but more difficult to handle. After information is transferred to a vendor, it is decrypted and stored legibly on his local machine. There is no way to prevent the merchant from misusing the information. For this reason, the customer has to establish a trust based relationship with every single vendor she wants to trade with. This leads to a situation where her personal information is spread to different Internet shopping servers. "The possibility of fraud over the Internet is only as likely as fraud from a transaction in person or over the phone, since the fraud is usually done at the end point", states Yvette Debow, a vice president at Jupiter. [Flynn, 1996]

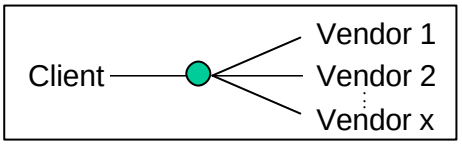

Figure 2: Client-vendor relationship

4.3 Scenario Two: Indirect Customer-Merchant Relationship

The Electronic Mall Bodensee acts as an electronic *intermediary* reducing the number of direct business partners. Instead of sending private information to many different merchants, the customer sends it only to the EMB. The resulting indirect relationship helps to preserve privacy.

An electronic mall provides a generic infrastructure for the different business partners. This can be compared to a real-world fair where exhibitors are supplied with general services such as electricity, water, telephone, logistics, etc. Typically generic services include payment systems (some malls even do the billing for the merchants), the establishment of certification authorities (key management), global directories (structured index where all merchants can be found), etc. All customer data is stored *only once* within the Electronic Mall. The Mall serves as a trustworthy intermediary. Its main business is handling information, so it should thus not compromise its reputation by handing information over to third parties.

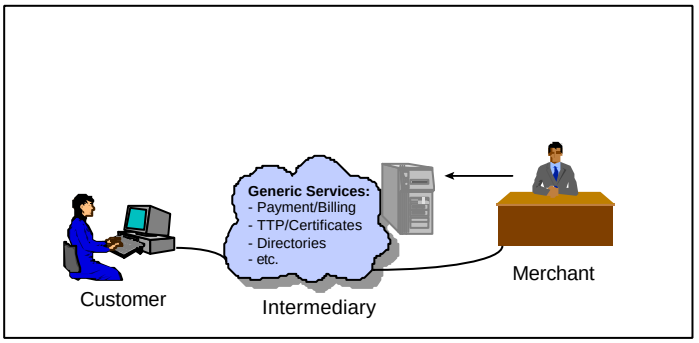

Figure 3: Indirect relationship helps to secure privacy

Electronic Malls, of course, are not the only possible intermediaries on the Internet. As companies discover new business opportunities, other types of intermediaries will emerge--for example, financial intermediaries (maybe banks), gateway services (e.g. secure electronic transactions (SET) gateway servers run by credit card issuers), trusted third parties (e.g. reputable companies, governmental agencies or telecommunication companies), and so on.

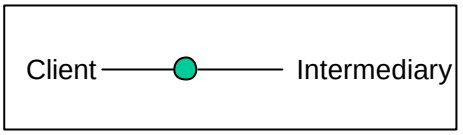

Figure 4: Reduced number of business partners

4.4 The EMB Platform

The following section deals with current privacy problems (especially for payment transactions) which still have not been solved on the Electronic Market Bodensee platform. Today, most commerce servers in the USA use SSL together with a 128-bit key to secure data transfer over the Internet. The big advantage of SSL is that it complies with the current most-used Web-browsers (of Netscape and Microsoft) and is therefore ready to be used on a large scale.

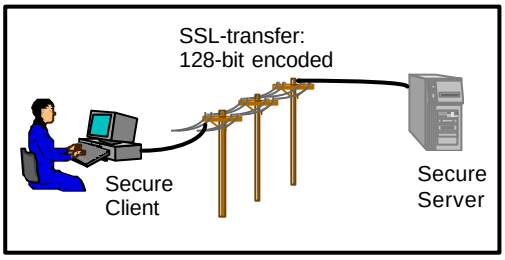

Figure 5: SSL

Since most Internet software is provided by American companies and there are strict encryption exportation restrictions in respect to length of keys used, most companies outside the USA face problems with guaranteeing transfer security to their customers. The Internet Privacy Coalition has recently asked for a relaxation of export controls on cryptography [Brier, 1996] thus helping to foster across-border trade.

The electronic shopping part of the EMB is implemented on the basis of the Netscape Commerce Server, an American product which uses 40-bit RC4 crypto for its exportable version. The 40-bit key has proven to be too short to really avoid eavesdropping. With an enormous amount of computer power some independent parties eventually managed to crack the crypto [Neumann, 1996]. European companies have therefore ultimately started to create own cryptographic systems. In Switzerland there are two competing systems under discussions to be used to secure payment transactions:

1. The BROKAT Solution

Brokat is a German company which recently developed a security solution for payment settlements. The product is Java-based and uses a 128-bit encryption key within the applet. The loading of the applet takes more than one minute, which makes the process quite time-consuming. The whole process takes place in two steps. First an identified connection is established and the applet is downloaded onto the client's PC with a standard web browser, as well as a standard web client (40-bit encryption). Once the applet is transferred the relevant payment information is encrypted using a 128-bit "Euro-key".

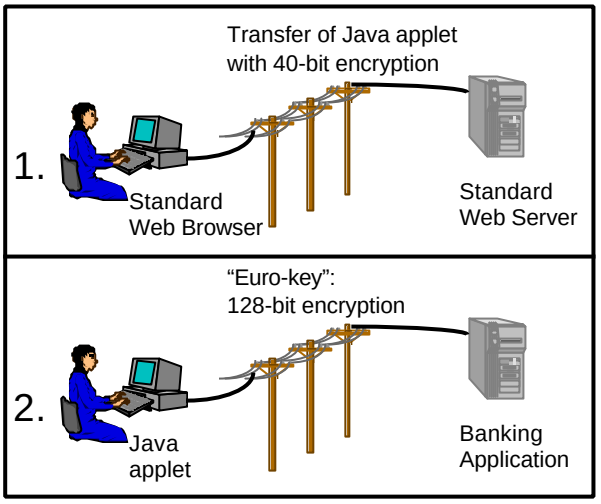

Figure 6: Brokat solution

2. SecureNet

SecureNet is a Swiss product developed by r3, a company specializing in security and encryption. SecureNet requires the installation of additional client software on the customer's local machine (r3 SSL HTTP Client). The software serves as a secure proxy which encodes the information using a 128-bit code. The SecureNet server also needs special software to be able to interpret the encoded information (the r3 SSL HTTP Server). The method is compatible with SSL (version 2.0) so that users with an original American web browser can use servers provided with SecureNet without installing the additional piece of software.

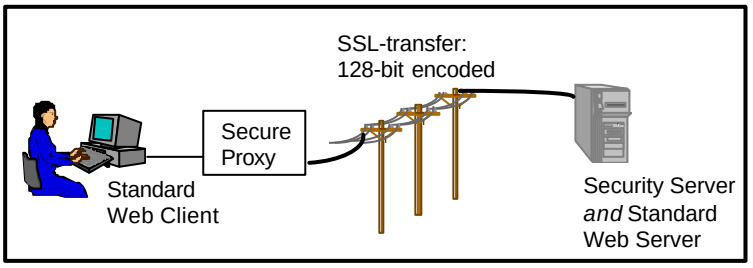

Figure 7: SecureNet ("SSL for Europe")

At the moment, most transactions are settled using credit cards. Consider as an example the above-mentioned regional wine shop. When a customer orders, let's say, two bottles of wine, she gives her credit card information, which is then transferred using the European 40-bit SSL encryption. The data it stored

legibly on the local EMB server in a SQL/Oracle database. Since the ordering process is not yet fully integrated into the merchant's order system, the order form is sent via FAX to his local shop. The FAX contains the product order as well as the credit card information. The customer, therefore, must rely upon the merchant as well as the provider of the EMB to handle her information confidentially.

Currently, an EMB project group is studying potential improvements that could be derived from using the SET-standard (Secure Electronic Transactions) payment protocol which VISA and MasterCard developed to enable secure credit card transactions via open electronic networks. GTE, IBM, Microsoft, Netscape, VeriSign and other important players supported the two credit card companies in developing SET as an open standard. Payment transactions which are performed using SET result in some big advantages regarding protection of personal customer information. These are:

1. Secured data transfer via encryption
2. Data integrity due to digital signatures
3. Authentication of card holder and vendor via digital signatures and certificates

The transaction system scrambles the credit card numbers so that they cannot be read when they are transferred across the Internet. The message is sent to an SET gateway server and the information is checked for validity. The bank (or credit card issuer) then authorizes the purchase and notifies the merchant (or the EMB in this case). The vendor only receives an okay message, but does not get to know the credit card information. The biggest advantages of this SET-concept are that no credit card information is revealed to any of the parties involved and no sensitive data is stored on local merchants' servers. Since SET works with certificates, there is need for the installation of trust centers (TTPs) as well as a certification hierarchy.

4.5 The EMB and Policy Vacuums

Electronic malls like the EMB open up many new possibilities that were never available before. For example, people all over the globe suddenly become potential customers for a "local" shop without ever leaving their country or even their own homes. Suddenly a wine shop in St. Gallen, Switzerland, for example, can potentially serve customers world-wide, instead of just people who happen to live nearby or tourists who happen to be passing through.

Also, in an ordinary physical mall it is not feasible to "track" the movements of all shoppers--recording where they stop, what they look at, how long they stay, what they buy, how much they spend, how often they come back, and on and on. With today's information technology, however, such detailed tracking of shoppers is possible; and the resulting information can be used to create revealing "personal profiles" on the lives, habits and preferences of individuals. In addition, in a physical mall, the customer retains a lot of control over the process of transmitting private information to merchants. By speaking or writing, the customer can deliver the necessary information directly, without having to send it through scores or hundreds of intermediate locations where it might be copied for fraudulent purposes. But information traveling through the Internet on its way to the EMB may go through many computers before reaching its destination.

How should these and other related privacy and security problems be solved? What policies and procedures need to be put in place to protect the privacy and security of data that flows to and from the EMB regarding thousands of customers? To answer these and many other privacy and security questions, the EMB is studying or trying to use various security measures and privacy policies. Should RC4 Crypto be used, or the BROKAT solution, or the SecureNet system? Should EMB serve as an *intermediary* between customer and merchant and thereby avoid spreading sensitive private information to dozens of merchants' computers? Should there be other types of intermediaries, such as banks, credit card companies, or government agencies?

4.6 The EMB and Wide Reflective Equilibrium

To answer a whole cluster of new privacy and security issues, the EMB must consider a complex fabric of already existing policies and rules--and it must formulate new policies of its own. What are the norms and practices in the Bodensee region of Europe? What international agreements and business practices are relevant or binding? The Internet links more than a hundred countries world-wide. Whose laws apply on the Internet? Whose definition of "privacy" should be used to formulate the new privacy policies? (The American definition and the European definition seem to be very different, for example.) Are there already accepted standards of business practice that can be stretched or reinterpreted to cover electronic malls like the EMB?

The creators of the EMB, their customers, the cooperating merchants and international business organizations, the regional and national governments involved are all engaged in a complex process of weighing considered ethical judgments, interpreting and adjusting old policies, and creating new policies. The aim of this complex process is to eventually formulate rules of conduct that will preserve and protect the security and privacy of personal data that flows through the EMB and makes Cyberbusiness possible in the Bodensee region of Europe.

5 Conclusion

The specific case of the Electronic Mall Bodensee graphically illustrates the complexity of social and ethical policy making that becomes necessary when the revolutionary technology of computing opens up vast new possibilities. It is clear that the decision process involved is much more complex than merely applying philosophical theories like utilitarianism and Kantianism to cases and dilemmas. Indeed, such an abstract academic activity may not take place at all; and in any case it would remain a very small part of the ethical policy-making process.

On the other hand, we believe that the "policy cluster model" of applying ethics which we present here goes a long way toward capturing *what really happens* in real-world situations. Because of this, we think the model is worthy of further development and examination.

References

Brier, Steven (1997) "How to Keep Your Privacy: Battle Lines Get Clearer" in *The New York Times*, January 13, 1997

Bynum, Terrell Ward (1997) *Information Ethics: An Introduction*, Blackwell.

Collins, W. Robert and Miller, Keith W. (1992) "Paramedic Ethics for Computer Professionals", *Journal of Systems Software*, Vol. 17, pp. 23-38.

Edgar, Stacey L. (1997) *Morality and Machines: Perspectives on Computer Ethics*, Jones and Bartlett.

Griffin, J. (1993) "How We Do Ethics Now" in A. Phillips Griffiths, Ed. *Ethics*, Cambridge University Press.

Johnson, Deborah G. (1985, 1994) *Computer Ethics*, Prentice Hall.

Langford, Duncan (1995) *Practical Computer Ethics*, McGraw-Hill.

Flynn, Laurie J., "Malls and Stores Find New Outlets in Cyberspace", *New York Times.*

Maner, Walter (1980) *A Starter Kit on Teaching Computer Ethics*, Helvetia Press and the National Information and Resource Center for Teaching Philosophy.

Moor, James H. (1985) "What Is Computer Ethics?" in Terrell Ward Bynum, Ed., *Computers and Ethics*, Blackwell. (Published as the October 1985 issue of the journal *Metaphilosophy*.)

Neumann, Peter (1996) "Risks in Digital Commerce" in INSIDE RISKS, *CACM*, Vol. 39, January 1, 1996.

Rawls, John (1971) *A Theory of Justice*, Harvard University Press.

Schmid, Beat (1993) "Elektronische Märkte" in *Wirtschaftsinformatik*, No. 5, 1993, p. 465-480.

Schmid, Beat (1996a) "The Development of Electronic Markets--A Swiss Perspective" in Klein, Stefan, Williams, Howard, *Emerging Electronic Markets: Economic, Social, Technical, Policy and Management Issues*, St. Gallen: Working Paper of the Competence Center for Electronic Markets, No. 23, 1996, pp. 5-26.

Schmid, Beat (1996b) 'Zur Konstruktion Elektronischer Märkte" in *Informatik/ Informatique*, No. 6, Dec. 1996, p. 5-10.

Spinello, Richard A. (1997) *Case Studies in Information and Computer Ethics*, Prentice Hall.

Spinello, Richard A. (1995) *Ethical Aspects of Information Technology*, Prentice Hall.

Tapscott, Don (1996) *Digital Economy--Promise and Peril in the Age of Networked Intelligence*, New York: McGraw-Hill, 1996.

van den Hoven, Jeroen (1996) "Computer Ethics and Moral Methodology" in P. Barroso, S. Rogerson and T. W. Bynum, Eds, *Values and Social Responsibilities of Computer Science*, Proceedings of ETHICOMP96, Complutense University Press, pp. 444-453. (Republished in *Metaphilosophy*, July 1997, Vol. 28, No. 3)

Zbornik, Stefan (1996) *Elektronische Märkte, elektronische Hierarchien und elektronische Netzwerke*, Konstanz: Universitätsverlag Konstanz GmbH, 1996.

Zimmermann, Hans-Dieter (1996) "The Model of Regional Electronic Marketplaces--The Example of the Electronic Mall Bodensee (EMB)". Accepted for publication in *Telematics & Informatics*.