Polite Computing: Software that respects the user

Brian Whitworth (bwhitworth@acm.org) New Jersey Institute of Technology, New Jersey

Abstract

This research proposes that legitimacy percepts underlie not only community laws but also politeness. If legitimacy is fairness, then politeness is being more than fair. If unfair acts destroy the fabric of society, then polite ones create it. Specifying legitimacy boundaries for computer based social interaction is proposed to be the baseline for designing systems that support politeness. Other conditions are that the parties can communicate, that action choices are clear, and that rights can be transferred. Computer system design could not only support online politeness between people, but also allow polite computing, where software respects user information ownership.

Introduction

Legitimacy is here considered a *social perception* of what group member actions are "fair" or right, and also socially beneficial. Our justice system seems a best attempt to implement this sense of fairness (Rawls, 2001). Legitimacy is then not just what everyone does, in a normative sense, but what makes society productive and adaptive. From Hammurabai's laws for governing Babylon, through to the Magna Carta (1297), the French declaration of the Rights of Man and of the Citizen (1789), and the United Nations Universal Declaration of Human Rights (1948), legitimacy advances have coincided with what can be called social "health", the total value generated for the individuals in a society by that society. As a society generates more value, it strengthens and grows, but if it does not, it weakens and falls apart. Social justice and community prosperity seem to correlate. Historical argument also suggests that legitimate communities prosper and endure, while communities that ignore it do so at their peril (Fukuyama, 1992). From a socio-biological perspective, fairness seems a lesson that societies must learn to evolve into larger societies, that can potentially generate more synergistic value (Diamond, 1998). Reasons are not hard to find, but mainly involve the intangible social value of trust leading to the tangible economic gains of cooperation (Ridley, 1996). Fairness means more people contribute more because they trust that they will not be cheated or abused. This means that in a fair society there is more work, more ideas, more research and more development. Also when systems are legitimate, and people trust the system, they self-regulate more. As they do not have to be forced to do things, this reduces police and internal security costs (Tyler, 1999). Psychology studies show people tend to avoid unfair situations (Adams, 1965), and may even prefer justice to personal benefit (Lind & Tyler, 1988).

If legitimacy benefits physical communities (Davis, 2001), the same logic applies to electronic ones (Schubert, 2000; Weltry & Becerra-Fernandez, 2001). This seems why articles on privacy, libel, copyright, piracy, trust, trespass, digital signatures, and other online legitimacy issues, regularly appear the Communications of the ACM. However though unfair acts, like stealing or lying. harm society they may give great personal benefit to those who do them. They are thus a temptation. Yet if everyone acted illegitimately, social interaction would no longer be adaptive. The recent cases of corporate fraud at Enron, WorldCom and others illustrate how fraud damages the social system we call "the market". Legitimate acts are adaptive for both the group and the individual, while illegitimate acts benefit the individual but make the social group less adaptive. If a virtual society needs legitimacy to be prosperous as much as a physical one, it seems sensible to carry forward the legitimacy concepts of physical society to virtual society. To re-learn the social lessons of history, often gained at great cost, in cyber-space, seems both foolish and unnecessary. To make this transfer means defining legitimacy and designing computer systems to support it (Whitworth & de Moor, 2002). From there, it is just another step to the positive generation of social value – politeness.

Politeness

If legitimacy is the boundary between fair and unfair, it is the minimum a good citizen should do. But it is not the maximum. Politeness is proposed to be when *a person, by choice, acts to be more than fair*. Thus while legitimacy is a group obligation not to destroy trust, one that is likely to be enforced by sanctions such as fines or prison, politeness is a choice to create trust. There are no laws and sanctions for politeness, as it is by nature voluntary. Just as it can be argued that criminal activity destroys the fabric of a society, so it can be argued that politeness creates it. Given this definition, politeness is not simply being nice or kind. For example, giving money to the poor is

kind, and benefits the community, but is not politeness. Nor is politeness about inter-personal relationships. For example, ringing your mother every day to ask how she is feeling may create a good relationship, but is not an example of politeness because it is not a group level issue. It is left up to the individual, as some mothers want to be called and some don't. Politeness, like legitimacy, is about *the relationship between the individual and the group*, and the types of interaction that make communities work. As a group level activity, politeness can apply regardless of whether you know the other person. For example, it is polite to let another go first, and this can be seen on the road where motorists let pedestrians cross, or allow another car to enter in a line of cars. In nearly all cases, the parties do not know each other personally. While politeness can be part of a personal relationship, it is more than just a way of getting another person to be good to you in return. In a large society, most cases of politeness are not reciprocal. Politeness allows resolution of interaction conflicts that would otherwise clog the courts with triviality, or escalate to physical conflict. While politeness is proposed to be based in legitimacy and public good, just as legitimacy can be formalized in law, so politeness can be formalized in "etiquette" – normative group rules of "good" behavior. However many see politeness as more than just fixed social conventions, as being a social good, and that is the view taken here. In sum, polite actions have two key properties. Firstly they are group adaptive, in that if everyone does them the benefits of social activity increase, and secondly, they are voluntary.

The online situation

However current online interactions often seem neither legitimate nor polite. Examples include Intel's inclusion of a trackable Processor Serial Number (PSN) in its Pentium III in 1999, Comet System's 1998 secret generation of "click-stream" data from people that used its software, Microsoft's Windows98 registration secretly sending system hardware IDs and user details back to Microsoft, and the suggestion that Microsoft's Media Player, bundled with Windows XP, quietly records the DVDs it plays and sends the information back to Microsoft (Editor, 2002). Our current performance implementing legitimacy in virtual environments seems at best weak (Privacy-International, 2002). Software adds, deletes, changes, views, copies and distributes information from <u>our</u> hard drive without considering to advise us, let alone request permission. For software to ask, not just take, seems the exception rather than the rule. The corporate view that "Your information belongs to us." seems based on software might rather than right. When we ask why software companies do such things, the answer seems to be "because they can". This approach is what leads some to suggest that we are becoming the "hunter-gatherers in an information age", people whom technology has returned to socially primitive times, where what rules is might not right (Meyrowitz, 1985, p315). The effect in virtual society of unfair activities is to reduce trust, which negates the immense possibilities the technology offers. For example, in 2001 President Bush decided not to use e-mail for any correspondence, and the basic reason seemed to be that he didn't trust it. If the President of the United States does not trust online activity, one can hardly blame the ordinary person for not doing so. Many people likewise do not trust online commerce, and hence do not participate in it. The potential benefits of technology are unrealized because of lack of trust. At one level it is an issue of security, of implementing control. But given security, the question still remains, who can do what? For example can a seller use "stealthware", that follows your mouse clicks as you surf the web, and adjust their offer price according to what they think you will pay? No amount of security can compensate for a lack of legitimacy, as police states around the world testify. There is developing an information inequality between buyer and seller, and while the seller knows more and more about the seller, from cookies and reading their browser history, sellers can be quite anonymous. This seems unfair. Until fairness is restored, buyers are likely to simply stay away. They have no reason to trust the online experience. Once implementation issues like security are resolved, legitimacy issues of who can do what are likely to loom large. If politeness is a way to increase trust, then it can be an antidote to this problem. By respecting their customers and their rights, rather than taking advantage of them, polite companies may engender the trust necessary for successful social interaction. But to do that requires changes in software code.

The power of code

Social requirements, like legitimacy or politeness, must be designed into computer based social systems because in them *software architecture constrains social interaction.* For virtual societies, who can talk to who, who sees what, who can create, change or delete what, etc, is all defined by lines of programmer code. Social software must define exactly who can do what, and so must assume what is socially good, a social world view, whether anarchy or dictatorship (Turoff,

1991). So while designers may not wish it so, a morally neutral virtual social world seems not an option (Brey, 1999). That we write the code that creates online interaction makes this social challenge different from previous ones. It is as if one could alter the physical laws of the face-to-face world. Once the virtual environment is created, traditional ethical, legal and social forces may be ineffective, e.g. if online actors are anonymous and invisible, there can be no social accountability. Imagine the effect of making people invisible in the physical world! If legitimacy concepts are not supported in software architecture design, they may not be possible at all. While originally the Internet seemed naturally ungovernable, it now seems that, like Anakin Skywalker, it can be "turned" the other way - to a system of perfect regulation and control (Lessig, 1999). To allow this to happen would be to deny history's lesson, that successful societies are fair

Legitimacy analysis

The method of legitimacy analysis, given elsewhere in detail, involves defining *who owns what* in the information system, and concluding what *rights of action* the system should support (Whitworth & de Moor, 2002). Table 1 suggests how common legitimacy principles can be translated into programmable system design requirements. For example, the legitimacy statement that people have a natural right to the fruits of their labor (Locke, 1690) is the basis of copy right. It leads to the IS design requirement that item creators have all initial rights to the item created (to view, delete, change or display). The benefit of this, and other legitimacy principles, is a trusted system, where for example people are not "cheated" of their effort, and so continue to create (Stefik, 1997). Privacy seems based on the idea that people own information about themselves, and release it only by choice. It has been well argued that *privacy is a public good*, as without privacy everyone is continually subjected to the stress of public scrutiny, and people cannot act freely (Regan, 1995). Legitimacy analysis allows principles like copyright and privacy to be translated into software design specifications. This, it is suggested, is critical to virtual

social prosperity. Two critiques of legitimate system design are that perfect legitimacy is impossible, and that legitimacy is relative. But if perfection were a condition of action we would have no society. Few would argue that society's laws are perfect, yet we strive to create them. In virtual, as in physical, communities, some legitimacy is better than none. Secondly, that laws vary between societies doesn't imply the purpose of legitimacy is arbitrary, only that it is a social problem that can be satisfied by more than one solution. Legitimacy analysis makes the social rights implicit in any system design explicit, allowing users and designers to be clear what rights are and are not supported. If legitimacy is inherent to politeness, legitimacy analysis is the basis for designing software to support online politeness.

Online politeness

In social interaction, politeness takes up where fixed rules or laws end. Being more flexible, it can cover the gray areas. For example, if two people in the physical world approach a door at the same time, there is a potential "collision", which can be resolved by force, by a law, or by politeness. The legitimacy basis is that the first to the door should enter first. But what

Physical Right	Virtual Right	Owner	Action(s)
Freedom	To control their persona	Person represented	Destroy, change
Privacy	To control personal information display	Person represented	Display
Property	To act on information object owned	Object owner	Change, view, destroy, display
Contract	To transfer/delegate all/some rights	Object owner	Transfer,delegate
Patent	To initially own a created object	Object creator	Create
Copyright	To display an owned item	Item owner	Display
Attribution	To attach/display item authorship	Object creator	Display author
Trespass	To exclude (prevent entry)	Space owner	Exclude
Sub-Letting	To allocate a sub-space	Space owner	Create sub-space
Publishing	To display in that space	Space owner	Display in space
Context rights	To display in an assumed context	Comment owner	Display in context
Informed consent	To know if being viewed/recorded	Person represented	View
Representation	To contribute to group action	Group member	Vote
Free speech	To contribute to group discussion	Group member	Display content

Table 1. Selected legitimacy concepts and IS rights

if both arrive at about the same time? If force is used, the result may be a fight, and the losing party may seek revenge. Such internecine conflicts are not good for the social group. Using a law requires an objective way to determine who was first, or lanes and stop/go signs as in roadways, which is not practical. A better solution is to leave it to the politeness of the parties concerned. In this case both avoid the collision by withdrawing gracefully, saying "excuse me", and one says "after you", and allows the other to proceed. Politeness prevents open conflict, which is resolved *by the local consent of the parties involved.* If politeness is *a form of social interaction* (rather than just being nice), it seems to require:

1. *Legitimacy baseline:* That defines the agreed rights of the parties in the situation
2. *Connected parties:* That parties are visible to and in communication with each other (Erickson & Kellog, 2000).
3. *Available action choices:* That the action choices of the parties are known and available to them.
4. *Delegation of rights*: That parties can formally or informally transfer rights to other parties.

In the case of two people approaching a door, the above are obvious and easily achieved. But in virtual interactions people are typically anonymous, asynchronous, restricted in action choices to what the software allows, and the passing of rights is rare. For example consider posting some creative work on the web, whether a poem, music, book or a class lesson. Currently, if another person can see it, they can also not only download it, and use it without permission, but even change it, for example to put their name on it, and distribute it as their own. Most software does not support digital creator rights in asynchronous distributed situations, though Acrobat is moving in that direction. The legitimacy baseline that an item creator owns the item they created is supported by the largely normative effect of the community concept of copyright. There is little code to support this concept. The next requirement for polite interaction is that the potential item user can communicate with the item owner. For example, encrypted owner contact information could be included in the document. Thirdly, the action choices need to be available – does the user want merely to view the item, or to distribute it? Finally there needs to be some way an item owner can transfer rights, which in a computer environment should be recorded. For example imagine seeing something online you wish to use. Rather than just taking it, select the "Request permissions" option of a pop-up menu. This would present the available action choices, which are those the owner is willing to offer. You choose to request permission to use the material in your teaching. After selecting Send, a request goes to the owner, who may be anonymous to you, and may grant the desired permission, giving both you and they a record of the agreement. Why bother designing complicated software to do this? Why not just let people take what they want? The answer, as always, is the public good. For the taker, it is a gain, but for the creator, it is a loss, and a society that does not support its creators depresses creativity. By contrast, if creators felt they had some control over what they offered, the Internet could be a place where one gained value, rather than a place where one had things stolen. It would be worth it to create, which is why copyright came about in the first place. The potential benefits of the Internet for creativity are more than we can imagine, but are currently not being realized because the Internet is not designed for social value. Even without software support, some people still ask permission to use material, using e-mail, but a system supported by software would be so much more efficient and effective. People want to be polite, but often lack the software tools to do so.

Spam, unsolicited electronic mail, illustrates many of the above points. Firstly it is a serious drain on productive use of the Web, as users must sift through the detritus of "junk mail" to find what is important to them. Sometimes key items are overlooked or deleted by accident amidst the flood of undesired messages. Technology allows a spammer to waste everyone's time at almost no cost to themselves. Compare how computers allow a cyber-thief to take a few cents from millions of bank accounts to steal a sizable sum. Spam steals not money but time, and when it does so from large numbers of people, the result is a community productivity loss of significant proportions. Though currently not illegal, it seems illegitimate (or unfair). How seriously people take it is indicated by the fact that some receivers ban e-mail from ISPs known to allow spam. Telemarketers seem the telephone equivalent of spam, generating unwanted telephone calls instead of e-mail. Again they benefit because their costs are low, thanks to technology, but the people whose lives are interrupted find them annoying time wasters. They destroy politeness, and surveys show that increasingly people simply hang up without so much as a goodbye. The inequity of the situation is clear when telemarketers, who have your home phone number, invariably refuse to give you theirs. You

cannot call them at home, or even call them back. The most pernicious of all are those where the caller is a machine. In New York state, a law has been passed that telemarketers must be registered, and users may request not to be called. This law is based on legitimacy concepts that are evolving, but have not yet been transferred to the online situation.

Legitimacy analysis asks who owns the personal address information kept on a spam company's database? The concept of privacy suggests that while the company may hold the information, the individual who the information is about also owns it. In other words, people retain rights to personal information even if it resides elsewhere (Nissenbaum, 1997). It is a joint ownership situation, which means that either party can withdraw the item. The company may remove a person from their database, and the person may remove their information from the company's database. It follows, if this is a right, that it would be polite to *offer* to remove people on every interaction, e.g. "To continue receive product information press YES To stop further mail press NO". Some companies do this, but it requires a different business model, one based on the customer as a partner rather than as an object to be used. Impolite actions presume a seller-customer battle, while polite product mail considers a willing customer better than one that resists, as resistors rarely buy anyway.

How does personal information get on spam company databases in the first place? One way is that it is simply *stolen,* for example from another transaction, or taken from another list. By contrast, suppose such companies needed to ask permission to use personal information. They would need to be identifiable and contactable, e.g. by being on a registered list. The action choices involved would be defined. For example giving a company your contact details, and the right to send product information, does not give them the right to pass on or sell that information to others. Giving a right does not give the right to further give the right. Finally, when the user gave permission, a copy would be kept on their hard drive. Removing themselves from the database at a later date would be merely a matter of recalling that permission and changing it. From a business point of view this could be good not bad. People are more likely to subscribe to a potentially useful service if they know they can withdraw. By comparison, people often buy things because they know they can return them. Currently users must exercise their choice by force, for example by email filters. Increasing amounts of bandwidth and computer time are devoted to transmitting messages people don't want, and don't even see, because they are moved directly into their trash cans. For example a great deal of Hotmail is spam. Some users solve the spam problem by changing their e-mail periodically to remove themselves from lists, but this also cuts previous social connections. Until recognized and dealt with, spam can be expected to be an increasing problem, both for hardware and people.

But a polite retailer might ask, how can customers even know of an offer unless you first tell them? This first offer should be regarded as a request to jointly communicate, an invitation to share ownership of the sent message. A natural requirement in joint ownership is that the other party be identified. Also if communication can only go one way, as with telemarketers, one is less likely to accept an offer to interact. Software could be designed to support these simple requirements. It could indicate which communications are from identified others, for example on a registered list, by immediately checking the list online. It could check which communications provide valid return addresses by sending a request to resend message with a unique user code, and rejecting any messages without it, i.e. it would only receive messages from senders who also receive. Finally it could truly reject, rather than place material in the trash can. Rejected spam messages would be returned to the sender unopened and unreceived, creating a problem for their disk space. For a spammer to satisfy these requirements, they would have to reveal themselves, which would makes them also susceptible to spam, and liable to receive back their returned spam. Moving to a more equal relationship increases the likelihood of legitimacy and politeness. When spam is everyone's problem, everyone is more willing to be part of the solution. Online society can make it everyone's problem by the design of software. Some may see this as a highly unlikely possibility – why should a company bother to be polite when they can bulk mail the world at virtually no cost? The main reason is that the community requires it for community prosperity. On a social-evolutionary level, the individually unlikely possibility of spam control seems a social inevitability. A society cannot forever allow a few senders to increasingly consume the time of the many for an ever decreasing benefit. A society that cannot prevent illegitimate acts will fail or stagnate. As societies evolve they must become more adaptive not less, as the less value social interaction generates for individuals, the less likely they are to participate in it. The alternative to a legitimate and polite online

society is no online society. Since it is unlikely the online community will allow this to happen, given the huge potential, ways will be found to introduce legitimacy and politeness into the online situation. This paper argues that this requires support at a software level, which requires that legitimacy and politeness be specified as IS design requirements. For businesses, inviting the customer into a partnership will ultimately be seen as better business than engaging customers in an electronic information war to gain an unfair advantage. The customer is not the enemy.

Polite computing

While people know how to be polite, programs, or the people who write them, seem slower to pick up the concept. Installation programs not only place information on your hard-drive, and in your registry, but may also install themselves in your Startup group and on the Taskbar, in a way users dislike. For example RealNetwork's Real-One Player adds a variety of desktop icons and browser links, installs itself in the system tray, and if the user is not very careful, commandeers all video and sound file association links. Every time Internet Explorer is upgraded, it changes the user's browser home page to MSN, and adds a series of items to the Links bar, all without asking. While browsing online, your screen real estate can be filled with unwanted pop-up windows, or pop-under windows that must later be closed. Programs can access your communication line, even initiating a dial up, without your permission. Every time we browse the web, programs place cookies on our hard-drive that we know nothing about to record what we do. The legitimacy of this situation is not hard to fathom. You paid for the hard drive, the screen, the memory and the communication line, so you should own it, and so ultimately have the right to decide what happens to it. It is supposed to be your "personal computer", so running programs cannot assume they have the right to access or use anything and everything they want to, simply because they can. For an installation program to assume it can do whatever it wants, is like the people who deliver furniture assuming they can help themselves to what is in your fridge because you let them in the door. Currently, only by third party tools like Black-Ice and Zone Alarm is a semblance of control wrested from unwilling programs. Many users are engaged in a war with their software, removing things they don't want, resetting changes they did not want changed, closing windows they didn't want opened and deleting e-mails they didn't want sent. It does not have to be this way. We could have *polite computing*, *where if software wants to change or do anything,* ***it asks first****.*

It can be argued that while our personal computer belongs to us, we are too ignorant to understand the intricate details involved for example in a typical install. However the same argument could apply to the installation of a security video system. It is up to the installer to explain the choices effectively. For software this means proper structuring or grouping of choices. Activities essential to application operation should be separated from optional changes. In these permissions, as in lawful interaction, the default is not to grant but to not grant a permission. A permission requires a positive act. The same support requirements listed earlier for person-to-person politeness can be applied to computer-to-person politeness. Firstly there must be a clear understanding of who owns what, that defines the rights of the situation. In particular, this means that it is clear that the user owns their computer. Second, the parties must be known and able to communicate. For software, this means making available a contact e-mail, telephone, address, listing on a register, or all of these. The software is not just software, but representing some party who is socially responsible for it, and what it does. Thirdly the actions involved in the situation must be clear. If a program is to place information on the registry, it should state what, where and for what purpose. These details need not be presented, but should be available for view, for example by pressing a Details button. In an asynchronous environment, they should also be stored. Finally permission should be given as a delegated right and a record kept. Both parties are entitle to a copy of this.

The Microsoft Paper Clip is an example of impolite computing. Suddenly, in the middle of some action by you, the paper clip took control of your cursor and asked if you needed help. While the goal seemed laudatory, many users disliked it, not only because it took over, but also because it was difficult to disable. There was no "go away" button on the paper clip itself. Changing the shape from a paper clip to a friendly wizard or a dog did not change the fact that it was like a rude guest who would not leave, no matter how many times you tried to ignore it. Most Word users remove it as soon as they learn how. The exception seems to be very new users, who welcome help when they don't know what they are doing. The view that we are children who need to be controlled by software that knows better than us is not a long term basis for human-computer interaction. Even when it is true, children grow up, and then want to take control of

what is theirs. They want some respect, and politeness is all about giving other people choices. A trend to polite computing would be a form of "growing up" by computer users, a part of online social evolution. This is not to say that polite software does not exist. It does. However because it is not an explicit system design requirement, it is neither consistent nor reliable. To be given a "seal of politeness"" software needs to be designed with that in mind. When software says "Please may I … ?", rather than just doing it, when it asks instead of just taking information, when it returns control of the computer to the person that owns it, then we will have polite computing. Who knows, one day when I willingly give permission to some trusted software to do something, the software may even say "Thank you", to which I will reply aloud – "You are welcome".

References

Adams, J. S. (1965). Inequity in Social Exchange. In L. Berkowitz (Ed.), *Advances in Experimental Social Psychology* (Vol. 2, pp. 267-299): Academic Press, New York.

Brey, P. (1999). The ethics of representation and action in virtual reality. *Ethics and Information Technology, 1*(1), 5-14.

Davis, R. (2001). The digital dilemma. *Communications of the ACM, February/44*(3), 77-83.

Diamond, J. (1998). *Guns, Germs and Steel*.: Vintage.

Editor. (2002, Sunday, Feb 24, section 4). Technology threats to privacy. *New York Times,* pp. 12.

Erickson, T., & Kellog, W. (2000). Social translucence: An approach to designing systems that support social processes. *ACM Transactions on Computer-Human Interaction, 7*(1, March), 59-83.

Fukuyama, F. (1992). *The End of History and the Last Man*. New York: Avon Books Inc.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Lind, E. A., & Tyler, T. R. (1988). *The Social Psychology of Procedural Justice*.: Plenum Press, new York.

Locke, J. (1690). *Second treatise of civil government* (Vol. Chapter 5, section 27).

Meyrowitz, J. (1985). *No Sense of Place: The impact of electronic media on social behavior*. New York: Oxford University Press.

Nissenbaum, H. (1997). Toward an approach to privacy in public: Challenges of information technology. *Ethics and Behavior, 7*(3), 207-219.

Privacy-International. (2002). *Big Brother Awards International*. Available: http://www.bigbrother.awards.at/org/ [2002.

Rawls, J. (2001). *Justice as Fairness*. Cambridge, MA: Harvard University Press.

Regan, P. (1995). *Legislating privacy, technology, social values and public policy*. Chapel Hill, NC: University of North Carolina Press.

Ridley, M. (1996). *The Origins of Virtue: Human Instincts and the Evolution of Cooperation*. New York: Penguin.

Schubert, P. (2000). *The pivotal role of community building in electronic commerce*. Paper presented at the Proceedings of the 33rd Hawaii International Conference on System Sciences, Hawaii.

Stefik, M. (1997). Trusted systems. *Scientific American, March*, 78.

Turoff, M. (1991). Computer-mediated communication requirements for group support. *Journal of Organizational Computing, 1*, 85-113.

Tyler, T. (1999, October 14-16). *Deference to group authorities: Resource and identity motivations for legitimacy.* Paper presented at the Society of Experimental Social Psychology Annual Conference, St Louis, Missouri.

Weltry, B., & Becerra-Fernandez, I. (2001). Managing trust and commitment in collaborative supply chain relationships. *Communications of the ACM, June/44*(6), 67-73.

Whitworth, B., & de Moor, A. (2002). *Legitimate by design: Towards trusted virtual community environments.* Paper presented at the Hawaii International Conference for the System Sciences, Hawaii.