Handbook of Research on Socio-Technical Design and Social Networking Systems

Brian Whitworth
Massey University-Auckland, New Zealand

Aldo de Moor
CommunitySense, The Netherlands

Volume I

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey · New York

Director of Editorial Content: Kristin Klinger
Director of Production: Jennifer Neidig
Managing Editor: Jamie Snavely
Assistant Managing Editor: Carole Coulson
Typesetter: Michael Brehm
Cover Design: Lisa Tosheff
Printed at: Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanbookstore.com

Library of Congress Cataloging-in-Publication Data

Handbook of research on socio-technical design and social networking systems / Brian Whitworth and Aldo de Moor, editors.
p. cm.
Includes bibliographical references and index.
Summary: "Every day throughout the world, people use computers to socialize in ways previously thought impossible such as e-mail, chat, and social networks due to emergences in technology. This book provides a state-of-the-art summary of knowledge in this evolving, multi-disciplinary field"--Provided by publisher.
ISBN 978-1-60566-264-0 (hardcover) -- ISBN 978-1-60566-265-7 (ebook)
1. Online social networks. 2. Internet--Social aspects. 3. Information technology--Social aspects. I. Whitworth, Brian, 1949- II. Moor, Aldo de.
HM742.H37 2009
303.48'33--dc22
2008037981

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter IV
The Social Derivation of Technical Systems

David Davenport
Bilkent University, Turkey

ABSTRACT

This chapter analyses the effect that social values have on the design of technical systems. Beginning with an examination of the role technology and accountability play in maintaining social order, it introduces the term "technology creep" to describe situations where conflicting viewpoints produce a technological arms race. Technology functioning in a social-order role inevitably supports one or other of the opposing views, so each side naturally uses it in an attempt to gain the advantage. Peace can be restored only by understanding the social dimensions of the conflict and finding a way of resolving them that is fair to all. The hotly debated issues of anonymity and copyright on the Internet are explored to illustrate this analysis, which, if correct, suggests that designers should consider not only a product's functionality, safety, its effect on the environment and users, but also non-users, especially those with different values. Awareness of the interplay between the social and technical realms will help optimize future socio-technical systems.

INTRODUCTION

This chapter examines the interaction between social values and technology, especially networked information systems. The basic idea is that technical products are always designed within a social context and so naturally embody the values, beliefs or viewpoints of the community that creates them. One is usually unaware of this, simply because most people share the same values. But, in cases where there are conflicting views, technology is often used by each side to "uphold" or promote their particular values. This can lead to a technological arms race in which the opposing camps continually create and improve their technologies in order to gain the advantage and so establish their views. Such conflicts are resolved only if: groups negotiate a peace deal that is fair and acceptable to everyone, a new technology is developed that diffuses the conflict, or one side "wins" outright (even though this may not be the optimal solution for everyone). Understanding such situations is only possible through consideration of

the broader socio-technical perspective, with the emphasis primarily on the social aspects, rather than the technological ones.

As an admittedly over-simplified example of this, consider the case of codes used to represent textual information in digital systems. The initial (commercial) development of computers was done almost exclusively in the UK & the US; a social context where the predominant language was English. It should come as no surprise, then, that the first standard code, ASCII (the American Standard Code for Information Interchange), only encoded characters in the English alphabet. Obviously, this caused difficulties in non-English speaking countries, forcing them to extend/modify the code to make it suitable for their languages, with the result that communicating documents between countries then became problematic. The difficulties were only resolved by countries/companies working together and defining a new universal code, the UNICODE, which satisfied everyone's needs. (Torsen, 2005) The situation still persists, however, in the use of English-only characters for Internet URLs.

The following sections look at why, in the case of opposing social values, technology tends to support a particular viewpoint, leading to a technical arms race, and explains why this is especially significant in the case of information systems. This qualitative analysis is then illustrated by two in-depth examples related to anonymity and copyright issues on the Internet. The paper concludes with some general recommendations for socio-technical system design and discusses the impact new Internet technologies may have on these.

ON THE ROLES OF TECHNOLOGY IN SOCIETY

If science is about understanding the functioning of the physical and social worlds, then technology is the application of this scientific knowledge to ease and enrich our lives. While it is well known that technology can sometimes have unexpected and undesirable consequences, and that its progress is difficult to predict, here the focus is specifically on cases involving technologies developed by groups with opposing values. To make sense of such situations, it is necessary to have some understanding of how society itself functions and manages the causes of conflict.

For the purposes of this chapter, take society to be a collection of individuals with a set of "rules" that govern their interactions. The individuals that comprise a society may change over time (as people are born and die, or as people join and leave the group); the rules, however, are founded on fundamental cultural values and while these will inevitably change, the change is likely to be much slower, perhaps almost imperceptible.

Societies survive because they afford benefits to individual members: food, shelter and security in the real world, interaction with people having common interests and goals in virtual worlds. In return, the individual members are expected to contribute to the society's well-being. The role and tasks an individual performs may be assigned by the group (especially in families and dictatorships) or may be left up to personal preference (as in most democracies.) Provided everyone plays a part, such social groupings can flourish. However, if one group or an individual benefits significantly more than other members of the community, problems can arise, especially if the imbalance is thought to have been gained unfairly. Injustice, whether real or perceived, breeds discontent and so threatens the well-being of the whole. How does a society maintain order in the face of often fickle human nature? One way is by force, but this is hardly a desirable option (except perhaps for the rulers) and, besides, given the inherent imbalance, maintaining control in this way can be very difficult. Better and potentially more stable, then, is a (free, democratic) form of society in which everyone is "equal" and generally "controls" themselves.

The rules that "control," govern or constrain, individual behaviour within a social group are of three forms: (1) personal ethics/norms, (2) physical & technological restrictions, and (3) a legal framework. (c.f. Lessig, 1999) Normally, individuals internalise

the ethics and norms of their society and so act in accord with them even in the absence of any outside influence or control. Technologies can make use of the constraints the physical world naturally places on individual actions to erect further artificial guides or barriers. Similar constraints can be erected using software to control interactions in the virtual worlds of the Internet. Finally, since it is generally impossible to erect barriers to handle every eventuality, it is also important to have a legal framework that acts as a catch-all. The law is an explicit statement of what is (or is not) acceptable and so, subject to due process, allows society as a whole to restrain individuals that threaten to undermine the rights of others.

Here, then, are two other roles that technology plays within society; a social-order role that serves to remind, guide, regulate or constrain individual behaviour, and a less obvious role, that of evidence provisioning in support of the legal process.

Whatever its role, technology often brings disproportionate benefits to particular individuals or groups. These may be the developers themselves or particular user groups, and may arise from the sales of the products or from the advantage the product gives to its users (for example, in terms of restrictions placed on others.) If the discrepancy grew too pronounced it might become a potential source of conflict, but things rarely go that far. Usually, other people either attempt to obtain a share of the benefits by doing the same thing (perhaps better), or try to develop alternate technologies and products which seek to redress the imbalance. Thus begins a sort of arms race in which groups compete, not just for a share of the wealth, but to establish a particular viewpoint. I term this "technology creep," a reference to the "feature creep" commonly observed in word processing and similar applications, and noting the irony between "racing" and "creeping".

A simple, everyday example may help clarify these notions. Consider the case of speeding. For safety reasons, the law requires drivers to keep within certain speed limits, especially in highly populated areas such as towns and housing estates. Most drivers understand the dangers and reduce their speed in such areas, even if not required to do so by law. However, there always seem to be instances where they "forget", and this is where technology comes to our aid. In its simplest form it may consist of speed limit signs that remind the forgetful driver; in some cases the authorities may construct speed bumps to slow vehicles down, or even redesign the road so it becomes impossible to travel too fast; or police may mount radar speed traps to catch the unwary, including unmanned ones which automatically record the evidence photographically. Of course in reaction to this, those motorists who believe they have a right to drive faster than the legal speed limit have developed various counter-measures. Some drivers signal other oncoming vehicles to warn them of the presence of a speed trap. More hi-tech methods involved detectors which picked up signals from the police radar guns and warned their users of the "danger" ahead of them (though such detectors are now generally illegal.) As more vehicles were fitted with GPS systems that helped drivers find their way around, information regarding the locations of speed cameras began to be included in them too, so drivers were again warned to slow down, not because speeding was dangerous, but so as to avoid a speeding fine. And so the technology arms race is perpetuated. It would be possible for vehicle manufacturers to fit devices to detect speed restrictions and automatically limit the vehicle to the designated speed, but such measures would be very unpopular and someone would likely find a way to deactivate them before long. Notice how each of these technologies embed the values of those for whom they are designed—on the one hand the speed traps and those who would seek to control dangerous drivers, and on the other those drivers who believe they should be free to determine their own speed and the information devices to ensure they retain that freedom—and how this leads to an escalation, each development being countered sooner or later.

Technology creep can have advantages. For one thing it can serve as a driving force for technological development (much as the ideological differences between the United States and Russia fuelled techni-

cal developments in weapons and space technology during the Cold War period.) (Evangelista, 1988) Sharing the improved technical know-how affords long-term benefits to all and through various wealth redistribution mechanisms (such as taxes), the short-term profits can be redistributed for the common good. However, technology creep also makes it extremely difficult to predict the consequences of any new technology. A relatively small, seemingly innocuous technical development, may provoke another small change, which leads to another and another, until the original idea has been changed profoundly and in ways almost no one could have anticipated. Such uncontrolled and essentially unpredictable technological change is bound to cause difficulties, at least for some sections of the community, and may thus threaten its overall stability. Moreover, even if some form of status-quo does appear to emerge, there is no guarantee that it is the most appropriate long-term solution, and having once "locked" society into it, it may be very difficult to change course (c.f. the adoption of the QWERTY keyboard, Liebowitz and Margolis, 1995). Understanding and resolving such issues necessitates looking at the bigger picture, involving social as well as purely technical concerns.

SOCIO-TECHNICAL DESIGN AND NETWORKED INFORMATION SYSTEMS

Socio-technical system (STS) research explicitly reminds one of the human social dimension that ought to be taken into account when designing systems involving technology. It recognises that technology doesn't exist in a vacuum, but affects those who use it and that they, in turn, affect its design. A socio-technical system, then, has a social component and a technical component, and both of these must be integrated and function together smoothly in order for the overall system to achieve its true potential.

In its early days, STS research was about humanising work "through the redesign of jobs and democracy in the workplace." (Mumford, 2000) It looked into the organisational issues involved in settings such as factory production lines, notorious for treating workers like robots. It developed a number of guidelines (Cherns, 1976), suggesting, for example, that if groups were given greater freedom and responsibility for their work, they would be more content and so more creative and productive. Later on socio-technical system design became concerned "with advocacy of the direct participation of end-users in the information systems design process" (Scacchi, 2004), the guidelines being updated (Clegg, 2000) to account for this new direction. Involving those who would be using the technology—whether factory production-line workers or information technology users—in decisions about its design and application, allowed potential conflicts to be identified and resolved before they caused any real problems. Today, such ideas find common expression in much engineering and management education.

This book is primarily concerned with the design of socio-technical systems that exist in the new virtual worlds of the Internet (Whitworth, 2006). The people who inhabit these worlds are those who inhabit the real world. They still have the same hopes, fears and flaws they always had, only the ways in which they interact with each other have changed. Thus, as business, government and individuals increasingly use the Internet to conduct real-world interactions, conflicts that arise in the virtual world can have potentially serious repercussions in the real-world. Consideration of social issues is thus equally important in both worlds if one is to maintain peace and prosperity, underlining the need for a socio-technical systems approach.

In the world of computers and the Internet the social-order function of technology is particularly significant because almost all of the interactions that take place are mediated by technology. This gives designers unprecedented freedom and power to organise and engineer the virtual society in ways that are often unique and simply unavailable in the physical world. This may not be immediately obvious, but consider what interactions are possible

with a bank's ATM machine or how the computer's operating system quite literally determines who can access what. If the system designer has decided you shouldn't be able to do something, you can't (assuming, of course, that there are no bugs in the program and that it can't be hacked!) This point was made by Lessig (1999) in "Code and other laws of Cyberspace", though, what the basis of this power is, how it should be exercised and whether or how it can be controlled are far from clear. As Hosein et al. (2003) also make explicit, system administrators and programmers are the new sovereigns, able to exercise absolute power over their domain.

To illustrate this analysis, consider two cases that clearly show the interplay between technology and social values, and the technology creep that ensues when there are conflicting viewpoints. The first case concerns the debate surrounding anonymity on the Internet and the second, the issue of copyright. To set the scene for these it is first necessary to discuss the role of accountability in cyberspace.

WHY ACCOUNTABILITY MATTERS

The virtual worlds of the Internet and the World-Wide-Web have transformed our lives. A great number of people in the developed world now have instant access to information about anything and everything; they can keep in touch with family and friends online, conduct business, do research, learn, be entertained, share their thoughts and contribute creative works to the milieu via blogs and social networking sites. But despite all these great benefits, it is not Utopia. Billions are still excluded from accessing this virtual treasure trove through lack of the necessary technical infrastructure. And there is an altogether darker side to today's cyberspace. The web has become infamous for gambling and pornography sites, and for allowing pedophiles, criminals and terrorists to operate relatively unhindered. Hacking, spam, viruses, phishing, identity theft, fraud and harassment are now commonplace. Recent estimates suggest that more than 50% of all email is now spam and losses from phishing were thought to be around $3.2 billion last year. (Gartner, 2007a) The cost of virus and similar malware infections was estimated by Computer Economics (2007) to be in the region of $13.3 billion dollars in 2006, down slightly from $14.2 billion in 2005, while over 15 million cases of the most rapidly growing cybercrime, identity theft, were reported in the US in 2006. (Gartner, 2007b) In less than a decade the atmosphere has changed. Such anti-social activities have gone from isolated teenage pranks to a multi-billion dollar sector controlled by organised crime.

The main reason for this explosion of criminal activity, I suggest, is the lack of accountability on the web. Of the three tiers of rules that govern an individual's behaviour (the ethical, the technical & the legal), the Internet currently lacks a properly enforceable legal tier. The reason is that the technical tier generally fails to provide the evidence necessary for a successful prosecution and this, combined with the difficulties of international legal action (Wall and Williams, 2007), make it ineffectual. First, though, it is important to understand just how crucial accountability is to the stability of a society. Consider what might happen if there were no accountability. You could rob a bank, steal a car, or kill the annoying neighbour, all without fearing any repercussions. Of course, others might try to steal your car or kill you too. Sooner or later someone would catch you off guard. Then it would be back to the law of the jungle—the survival of the fittest—everyone would live in fear and no one would stay on top for long. The only way to avoid such a scenario is for everyone to agree, for their own sakes, that they will not kill, or steal, or do to others what they would not want done to themselves. There are three alternatives: (1) rely on everyone to abide by this agreement, (2) create barriers making it impossible for anyone to break the agreement, or (3) agree, individually and collectively, to protect each other against any who would break the agreement. Sadly, human nature seems to rule out reliance on (1) and (2), so (3) is our only real hope. In other words, society (subject to appropriate safeguards) must be able to restrain individuals who would harm others.

Whatever the philosophical merits and problems of Social Contract Theory, (see Rawls, 1999; Skovira, 2003), all that is relevant here are the practicalities of ensuring social stability. As already shown, most real-world societies sensibly take a belt-and-braces approach by combining all three options in order to hold individuals accountable for their actions, but the point remains, (in the absence of moral perfection) societies must ultimately rely on (3) and, on the Internet, enforcing such an agreement is extremely difficult.

Viruses, spam, phishing, identity theft, hacking and even piracy, then, are all symptoms of this lack of accountability. Each of them has given rise to its own technology creep as the various groups battle it out. For example, applications that check incoming emails and files for viruses now have to be updated daily to combat newly emerging threats, with firewalls to restrict unwanted intruders, and virtualisation to limit the damage if all else fails. Spam filters have gone from simply rejecting email based on the source address, to scanning the text and using Bayesian reasoning to estimate the likelihood of it being spam rather than a genuine communication. Spammers have responded by automatically adding extra words to their emails to bypass the filters, and by embedding their message in image or sound files. Social filtering is now seen as the best hope of combating spam (Whitworth and Whitworth, 2004). When it comes to the social values driving this technology creep, it seems difficult to justify virus writing, phishing, or identity theft. Those who indulge in such activities do so for unjust personal gain or seem intent on disrupting society. It could be argued in some cases that "one man's spam is another man's advert", but clearly some form of compromise is needed if the current deluge is to be stemmed. In the case of copyright infringement there do appear to be justifiable viewpoints on both sides of the debate. These will be examined in detail shortly, but first consider the arguments against accountability put forward by those who believe in anonymous communication.

ANONYMOUS CONCERNS

Why can't Internet users be held accountable? Why shouldn't they be accountable? Part of the answer undoubtedly lies in the arguments of those who believe in anonymous communications and their influence over the technical infrastructure of the net. Anonymity is seen as the ideological opposite of accountability, a dichotomy of views that leads to another instance of technology creep as the two sides battle it out for supremacy. The following sections illustrate the resulting technical to and fro, and hint at the deep social debate that underlies it.

Technological Aspects

Every computer on the Internet is assigned an IP address, a number that enables the network (TCP/IP) software to efficiently route messages from one machine to any other machine on the planet. The details of how this packet-switching network functions need not concern us here, except to note that each packet (message part) that is sent, includes the IP numbers of both its source and its destination. Intermediate routing machines examine the destination address to send the packet in the right direction. When the message arrives at its final destination, the IP number of the source is available in the packet, should a reply need to be sent back. For all practical purposes, this is the only information the destination machine has about the sender of the message (and it is thus frequently logged—recorded—for security purposes).

In fact, there is no guarantee that the source IP number is actually correct. Since none of the routers ever check it, one way to remain anonymous is to fake (spoof) the source address. Another option, one that allows interaction between the source and destination, is to use a proxy server. Proxies work by exploiting the packet-switching nature of internet communication. The client (source) machine sends its request for a particular resource (on a destination machine), as data embedded in a request sent to the proxy. The proxy machine extracts the embedded request and sends it to the destination machine.

The destination machine can send any reply it may generate back to the proxy, which in turn forwards it back to the client machine. The destination machine sees only the proxy, never the client, which thus remains conveniently anonymous (especially since such proxy servers rarely keep any records).

Requests to a destination machine (be it for email, ftp files or web pages, etc.), will frequently require it to identify (authenticate) the user, to ensure it delivers only items that the user is allowed (authorised) to access. This might be done by checking the IP address of the request's source (enabling access to be restricted to particular machines), and/or by asking for a username and password, or an encrypted certificate (key). User accounts (identities) may be individually created for users known to the machine's owner(s) and the password/key (credentials) be given to them in person. On publicly accessible Internet sites this is rarely possible, so user accounts need to be created on-demand, with users often being asked to provide a validated email address or a certificate issued by a trusted third party, to reduce the number of bogus accounts that are created. Users that misuse a website can be banned or their account deleted, but if creating a new user account is quick and easy (as it usually is), this doesn't actually resolve the problem. How identity can be reliably established on the web, especially in the face of concerted attacks, is an important research area (Hardt, 2005).

One of the most significant security-related technical innovations is undoubtedly public-key encryption. It enables communications to be encrypted so as to guarantee they remain private and non-repudiable. It is also used as the basis of so-called digital certificates, that go some way towards establishing trusted identities. Lessig (1999) pointed to potential dangers of such certificates, while Hosein et al. (2003) discuss regulatory aspects of Microsoft's CAPI. Other technical developments of late include a number of more sophisticated versions of the anonymous proxy server, including onion-ring routers (such as TOR), which attempt to overcome the proxy's vulnerability to statistical pattern analysis of input/output packets by utilising multiple proxies, possibly in different countries, making it practically immune to legal (political) interference. Another recent addition to the anonymizer's arsenal has been software that explicitly removes records of browsing, email, etc., from a user's machine when they finish their work, especially important (to the paranoid) if surfing the web from a public machine. And there is now the added complication of wireless (wi-fi) networks that can allow anyone to join the network and then leave without trace. Such "removal of evidence" severely handicaps computer forensics; a science which is improving, but still very limited in comparison with its real-world counterparts (Panda, Giordano, and Kalil, 2006.) There is no obvious end to this technology war, a clear indication that a fundamental values dichotomy exists. These social aspects are now considered.

Social Aspects

Many of the early netizens were overtly anti-establishment and anti-big business (Barlow, 1996.) They believed in democracy and freedom of speech, and saw anonymity as the only way to ensure that governments could never interfere with or restrict these rights. They claimed that anonymous communications also enabled political dissidents and whistle blowers to speak out freely, and pointed to the advantages it had for ordinary citizens to discuss their personal, medical or family problems with others, without fear of embarrassment.

Such arguments have proved extremely forceful. If you are truly anonymous, then obviously (by definition), the state cannot locate you and hence cannot stop you expressing whatever opinion you wish. Try as he might, Big Brother cannot interfere. The cloak of anonymity naturally safeguards freedom of speech (expression) along with democratic rights to unfettered political discussion.

Opponents of anonymous communications take a slightly different view, relying on accountability and openness to ensure democratic freedoms. While acknowledging that anonymity may well encourage ordinary people to speak freely about their personal problems, and about political and

commercial wrongdoings, they question how much credence should be placed in such messages. Without knowing the originator of a message there is no way to judge its validity and it would surely be unwise to commit lives or sully reputations without more substantive verification. Besides, there are legitimate limitations on the right to freedom of expression; one cannot make false accusations against another or incite others to violence (Mill, 1860.) To redress the balance and restrain individuals who would cause harm to other members of society, it is vital that they can be found, i.e. that they can be held accountable. Indeed, the right to free speech itself presupposes that the speaker can be held accountable. Its purpose is to protect the speaker against those who would silence them, be they the moral majority, big business or the government. Those who oppose anonymous communications also point to the fact that, were such communications available, they could also be used by the state (Davenport, 2002.) It was a passionate belief in democracy and free speech, and a deep distrust of government, that led to calls for anonymous communications in the first place, but the result may just have the opposite effect. A government—legally—able to act anonymously would be an extremely dangerous proposition, and the same is true for religious, business and criminal groups, as well as individual citizens. Better, claim the proponents of accountability, to rely on openness and honesty, and retain the safety net offered by the legal tier, than to risk a spiral into anarchy (for better or worse).

Before leaving the topic of anonymity, it is appropriate to mention the issue of privacy, a concept that has further confused the debate over anonymity. How much privacy individual members of a society enjoy is entirely up to the community. The full range of privacy options is observable online. Some forums afford no privacy whatsoever; the messages, usernames and originating IP numbers being permanently visible to everyone on the web. Others may log the IP number, but make it visible only to members and/or the system administrator, while other (more chat-like) systems may keep no records whatsoever. While there are real world communities that afford members no privacy at all, citizens of most modern (western) democracies have come to expect a certain level of privacy in their affairs. In particular, they expect their communications to be confidential—a right written into the UDHR—thus, in most countries, illegal wiretapping/eavesdropping carries heavy penalties. Of course, the concerned citizen can always encrypt the contents of their message, so this is not really an issue for those on either side of the divide. However, when public messages are posted to online forums, privacy advocates insist that the origin of the message should also remain hidden. To be truly anonymous, communications must thus stop anyone from knowing who is communicating, rendering such communications utterly private. In contrast, accountability demands that the originator of a message be traceable, which potentially entails some loss of privacy. Accountability does not, however, require communications be traceable by everyone; even the recipient of a message need not know or be able to determine its origin. All that is required is that the courts, if necessary and subject to due process, be able to locate the sender (or at least the sending machine, further evidence usually being needed to determine who was actually using the machine.) While everyone might agree that this affords a degree of anonymity appropriate for whistle-blowing and the discussion of personal problems, fundamental differences remain (though perhaps less acutely in a post 9/11 world obsessed by the threat of terrorism).

COPYRIGHT MATTERS

The general dislike of commerce and the ethos of sharing that grew out of the early days of the web, has led to another conflict, one undoubtedly fuelled by the lack of accountability, but one in which there are also genuine differences of opinion. Today, many web users see nothing wrong with freely sharing copyrighted software, music and even films, yet to the creators of such intellectual "property" those users are thieves who are robbing them of their

livelihoods. Illegal copying of intellectual works, especially music and software, has reached epic proportions in recent years. Estimates by the Institute for Policy Innovation put global losses in the music industry at around $12.5 billion every year (RIAA, 2007.) The Business Software Alliance (2006) survey showed global software piracy running at around 35% and costing an estimated $40 billion. The following sections look at the technology and social aspects of this conflict.

Technology Aspects

Digital technologies now facilitate the copying and distribution of all forms of intellectual property at essentially zero cost, disrupting the established system which relied on the sale of physical copies of the work for its income.

Not surprisingly, the software industry was the first to experience piracy as a result of the new technologies. It applied the obvious solution, a software "key" that the user had to enter when installing the program and without which the program simply could not be used. This naturally frustrated the tech-savvy, who responded by sharing keys and developing program patches (cracks) that circumvented such copy-protection schemes. A running battle ensued (and continues to this day) with software manufacturers developing ever more complex protection schemes and the pirates taking up the challenge, developing their own technologies/tools with which to undermine whatever measures the manufacturers came up with. (Barber and Integralis, 2001) Physical keys, in the shape of hardware dongles that had to be plugged into the computer for the software to work, were also tried, but failed to gain user acceptance. Hardware manufacturers even tried producing processors with unique, software readable ID numbers etched into the silicon, but these were quickly removed as a result of privacy concerns (McCullagh, 2000). The Internet has opened up new possibilities. For example, Microsoft's XP operating system requires an activation key which the company checks and records online, ensuring its uniqueness. Similarly, their Genuine Advantage program validates the software is a legal copy before allowing updates to be downloaded. Online multi-player games have also successfully exploited a subscription service-based model.

The longer-established music industry has been hard hit by the advances in technology. From pressed vinyl records which were very difficult to reproduce, through to cassettes and CDs, which consumers could record themselves, the industry's business model remained unchanged. Piracy grew steadily once recording equipment became widely available, but illegal copying on a commercial-scale was limited since creating and shipping physical goods was comparatively risky and expensive, and, until the advent of digital technology, the quality of such copies was always relatively poor; it was thus only the comparatively high end-user prices that made the risk worthwhile. The film industry had experienced similar difficulties with the pirating of its video cassettes, so when DVDs were developed they tried to make sure that they were encrypted and that consumer equipment would only play DVDs for their particular region. It was not long before computer geeks managed to break the encryption, allowing legal & pirated DVDs to be played on computers. Fierce legal battles ensued with no obvious winner (Simons, 2000). Besides, it is impossible to stop copying by such means, because of the so-called analog hole. Music has to be decoded for legitimate users to listen to it and at that point it can be re-recorded. The film industry suffers a similar form of piracy, whereby movie-goers sneak camcorders into a cinema, secretly record the latest blockbuster movie and then burn it onto a CD and sell it, or share it with other fans on the web. Computer programs are also susceptible to the same fate when run on virtual machines.

The real revolution and another bout of technology creep began with developments in compression technology. Music compressed with the MP3 algorithm was practically indistinguishable from the original uncompressed version, yet occupied only a fraction of the space. Suddenly it became viable for consumers to store and play music on their computers

and new portable audio (MP3) players. They could compile collections of their favourite tracks and "share" them with their friends. As storage costs fell and communications speeds rose, huge repositories of music (software and films) were created on remote Internet servers from which everyone could (often illegally) download whatever they wanted. When the music industry took legal action to close down such file-servers, music sharing simply went back underground. MP3s were kept and swapped directly between users' personal machines instead. For users, the only problem was locating another user with the files they wanted. This difficulty was solved by Napster, which automatically created a centralised index of the music files stored on each of its users' machines (McCourt & Burkart, 2003.) Users could then search this index and simply click on the file they wanted to start downloading, peer-to-peer (P2P), from whichever users happened to be online at the time and, if the connection happened to break, Napster could automatically continue downloading from the next machine it found available. Being a centralised system, however, Napster too was vulnerable to legal action and was eventually closed down, but not before millions of (new, normally law-abiding) users had developed a taste for free music. As a result, it was not long before distributed P2P indexing systems, more resistant to legal action, were being developed. Some of the more unscrupulous copyright holders flooded download services with virus files or music files that were corrupted, so additional "quality ratings" began to be added to these indexes.

The same technology that facilitated illegal sharing also made it easier for publishers to locate & prosecute users, at least the relatively unsophisticated ones who failed to take precautions to hide their identity. But taking 10 year olds to court only served to alienate users. Realising they were losing the battle, music companies changed tack and tried to encourage legal downloading. By making it cheap and easy for music lovers to legally purchase individual tracks from an album, usage of online services such as Apple's iTunes exploded and their portable player, the iPod, became a modern icon, spawning numerous imitators. But there was a catch; the downloadable music was often encrypted and could only be played on particular machines. Digital Rights Management (DRM) software requires a special certificate/key to decrypt the music for the user, and so harks back to the initial attempts by the software industry to protect its products using software keys. Not surprisingly, DRM has drawn the same response; angering users and challenging hackers. To make matters worse, some publishers used the control that DRM gave them to introduce additional restrictions, for example, limiting the number of times the media could be played or removing the ability to make backup copies or play it on a different machine. Public outcry over such restrictions on "fair-use" has already persuaded some publishers to remove DRM controls entirely. (Anderson, 2008 & Stone, 2008).

Social Aspects

Underlying these battles are two conflicting views of the role of copyright in the information age. Copyright, as outlined in the Berne Convention, assigns to the creator of a work the moral right to claim authorship and the commercial right to restrict distribution and reuse, and to claim payment for such. Commercial rights can be transferred to a third party. For hundreds of years, artisans only got paid for the work itself, for live performances or, for a lucky few, by commission from a rich patron. The technology to record and mechanically replicate performances, enabling artisans to claim income from the sales of such recordings, is a comparatively recent and very successful innovation. However, today's digital technologies have made obsolete the business model that relied on the distribution of physical copies of the media, leaving artists and their representatives (publishers) desperately trying to protect their livelihoods. Understandably, copyright holders who believe they have a moral right to be rewarded for their work, attempt to stop illicit (unpaid) copying of their creations by whatever means they can. This has included technical options (such as DRM), as well as legal action (enacting and aggressively enforcing

ever stricter copyright laws, such as the DMCA), and awareness campaigns designed to educate the public (especially children) to the plight of artists. None of these measures seem to have had much real impact, other than alienating customers.

The protectionist approach contrasts sharply with the perception of cyberspace as a "free-for-all" frontier world that cannot be regulated. Those on the other side of the divide fall into two broad categories; the "pirates" who share by infringing copyright, and those who use copyright to protect the right to share.

There are a number of reasons why the illegal sharing of music, software, films, etc. continues. For one thing, most people don't view it as stealing. What could be more natural than sharing things you like with friends in the comfort and privacy of your own home? No one will ever know; on the web you are anonymous! Besides, it isn't really stealing, is it? After all, copying doesn't deprive the creator (copyright owner) of the work itself, only the income they might have made from that particular copy. There is also a general perception that prices are too high. Buyers typically contrast the fortunes accumulated by pop stars, publishers and software CEOs, with the low cost CDROM or downloaded file they get for their hard earned cash, and feel little sympathy or inclination to add yet more to the coffers of the super rich. Music lovers usually appreciate the creative effort of the musicians themselves and their need (right) to earn a living from their talent, but can still find it hard to justify the price being asked. While some of those illegally downloading do have the money to legally purchase the music (games, software, videos, etc.), many do not. Prices are rarely adjusted in line with income so that the poor, whether in the developed world or less well-off countries, simply cannot afford them. Of course, this doesn't justify theft, but, then, it isn't exactly stealing, is it?

But piracy is not just a matter of economics. It has already been noted how DRM software has undermined existing notions of "fair-use" and, as some users have found to their cost, even if you do pay (via subscription service or DRM keys), your rights may vanish if, for example, the service goes out of business or simply decides not to support the product any longer (Thompson, 2007.) It was a similar worry, combined with the lack of any right to modify software (Williams, 2002), that led to perhaps the most significant change in this area, the Free Software Foundation/Open Source Software (FOSS) movement. The FOSS community demonstrated a completely novel form of software production founded on mutual help and sharing. The Internet provided the platform necessary to bring people together for such egalitarian purposes. Copyleft licenses re-purposed copyright law to ensure that users always retained the right to have and modify a program's source code. While such software can usually be downloaded and used for free, this is not essential and programmers can chose a form of license that still requires users to pay. Creative Commons licenses extend this notion, promoting the reuse of all forms of intellectual work, so sparking similar movements in other areas.

The web may have produced a new breed of artisans, with websites such as Wikipedia, Blogger, YouTube and Flickr, but it has not yet entirely solved the problem of how they can make a living from their talents. Commercial concerns such as Google are pushing an ad-sponsored approach, giving websites a proportion of income from targeted advertisements embedded into the site's web pages. Another option for musicians in particular, is to get money from live concert performances, relying on websites such as YouTube for free publicity and distribution. Programmers too, can benefit from contracting jobs that may come about through contributions to open source projects. All this, however, is simply a return to the original old-world business model. In the new Internet-connected digital world there is another more novel option gaining ground. A quiet revolution is underway (Davenport, 2005) as more and more websites begin to sprout "Donate" buttons (generally linked to PayPal or Amazon's services.) Visitors who find what a site offers (be it information, software, music, etc.) useful or enjoyable, can easily contribute whatever monies they feel are appropriate. This solves the dilemma faced

by users who are unable to afford or are unwilling to pay the fixed asking price, perhaps because they are unsure of the benefit they will derive from the work. Encouraging such positive behaviour could help make piracy a thing of the past and open up new markets allowing everyone young and old to gain some legal (and taxable) income from their artistic talents.

DISCUSSION

Social values and beliefs pervade our actions and our artefacts, but this usually only becomes apparent when there are opposing viewpoints. It then manifests itself in technology creep, the technical arms race that ensues as each side tries to promote its views through the creation and use of technical products. Technology can help support a particular viewpoint because of its role, alongside ethical and legal means, in maintaining social order. This paper examined this relationship and offered an analysis of it that emphasized the importance of accountability in maintaining social stability. Two cases involving conflicting value systems were used to illustrate this: anonymity and copyright. Analysis of the conflict between anonymity and accountability is particularly revealing. The lack of accountability on the web enables cybercrime to continue unabated and so threatens social order. Yet efforts to change the web's infrastructure to allow evidence necessary for law enforcement to be gathered are frustrated by those who see anonymity as society's only safeguard against a potentially all powerful state. In the case of copyright, itself doubtless fuelled by the lack of accountability, instances of technology creep are especially obvious. Of particular interest though, is the use by both sides of mixed forms of regulation, not just technological, but legal and ethical as well. Despite new technologies being responsible for the (re)emergence of the conflict, the case of copyright is nevertheless striking for the novel, socially beneficial (technical) solutions that appear to be evolving.

If this analysis is correct, then designers must recognise that the conflicts are fundamentally social:

"Future socio-technical designers may face questions of what should be done, not what can be done. There seems no reason why software should not support what society believes." (Whitworth, 2006, p537)

This paper suggests that designers already face such choices and that the real challenge is to be aware of the values underlying them, since society is rarely homogeneous in its views. This is even more important given the special role that technology, especially information technology, plays in maintaining social order. Designers have always known that they should consider the needs of the user when determining a product's functionality. They gradually became aware of the need to consider safety issues and, more recently, environmental concerns. Socio-technical design explicitly reminds them that other social concerns must be included too; that is, designers must consider not just the users of their technology, but others in the community. Our analysis emphasizes the need to include those who may have opposing values/views, something already very apparent in the case of security.

This paper has focused primarily on information technology and its role in building stable, harmonious societies, but it is clear that one must attend to and view the ethical, technical & legal forms of control together. "Social technologies" need to be an integral part of the STS design world.

Postscript: STS Design in a Web 2.0 World

The infrastructure of today's web is the result of serious engineering design, much of it done by companies and research institutions. Increasingly, though, applications that run on this foundation are being built very quickly by groups that are not fully aware of the effects their programs may have. Rather than being carefully crafted, software today seem-

ingly just evolves! How relevant is STS design to the world of software development opening up with Web 2.0 (O'Reilly, 2005); a world where everyone contributes, where users are developers, a world of perpetual upgrades with shorter and shorter development cycle times; a world changing so rapidly that making sense of it is difficult enough, much less controlling it.

Major Open Source projects (such as, Apache, Firefox, etc.) still tend to have a relatively small core group of developers who provide stability and direction. They are often experienced engineers who understand the importance of systems that are amenable to change and thus strive to provide a secure modular platform upon which others can safely build. The FOSS community has gradually developed tools and techniques (e.g. CVS, testing frameworks, bug tracking systems, CMS, etc.) to help ensure their efforts remain viable, but this can only continue if the platforms themselves remain open to everyone.

Provided people remain vigilant, STS principles will continue to serve us well and hopefully permeate engineering practice. If the core developers do their "job" as best they can, having lots of people watching over the results should help ensure appropriate solutions. The so called "Wisdom of Crowds" (Surowiecki, 2005) may not provide absolute control, but at least with many people involved and able to see any conflicts that arise, new innovative solutions to these conflicts are likely to be found much sooner.

ACKNOWLEDGEMENTS

The author would like to express his gratitude to the editors, Brian Whitworth and Aldo de Moor, and to Robin Turner, Murat Karamüftüoğlu, Markus Schaal, William Sawyer, Fazli Can, Eray Özkural & Derya Davenport, for helping to clarify the arguments and shape the paper.

REFERENCES

Anderson, T. (2008). How Apple is changing DRM. *The Guardian*. Retrieved May 22, 2008 from http://www.guardian.co.uk/technology/2008/may/15/drm.apple

Barber, R., & Integralis, A. (2001). Hacking Techniques: The tools that hackers use, and how they are evolving to become more sophisticated. *Computer Fraud & Security*, *3*, 9-12. Available online as doi:10.1016/S1361-3723(01)03014-7

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Retrieved January 15, 2008 from http://www.eff.org/~barlow/Declaration-Final.html

Business Software Alliance (2006). Retrieved January 15, 2008 from http://w3.bsa.org/globalstudy/

Cherns, A. (1976). The Principles of Sociotechnical Design. *Human Relations*, *2*(9), 783-792.

Clegg, C. W. (2000). Sociotechnical Principles for Systems Design. *Applied Ergonomics*, *31*, 463-477.

Computer Economics (2007). Annual Worldwide Economic Damages from Malware Exceed $13 Billion. Extract from the *2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other Malicious Code*. Retrieved January 15, 2008 from http://www.computereconomics.com/article.cfm?id=1225

Davenport, D. (2002). Anonymity on the Internet: Why the Price may be too High. *Communications of the ACM*, *45*(4). Retrieved January 15, 2008 from http://doi.acm.org/10.1145/505248.505267

Davenport, D. (2005). *Free Copyright*! *Refundable Donations*. Retrieved January 15, 2008 from http://www.cs.bilkent.edu.tr/~david/papers/FreeCopyrightRefundableDonations.doc

Evangelista, M. (1988). *Innovation and the Arms Race: How the United States and the Soviet Union develop New Military Technologies*. Ithaca: Cornell

University Press. 300pp.

Gartner (2007a). *Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks*. Retrieved January 15, 2008 from http://www.gartner.com/it/page.jsp?id=565125

Gartner (2007b). *Gartner Says Number of Identity Theft Victims Has Increased More Than 50 Percent Since 2003*. Retrieved January 15, 2008 from http://www.gartner.com/it/page.jsp?id=501912

Hardt, D. (2005). Identity 2.0. Proceedıngs from *OSCON 2005*. Retrieved January 15, 2008 from http://identity20.com/media/OSCON2005/

Hosein, I, Tsiavos, P., & Whitley, E. (2003). Regulating Architecture and Architectures of Regulation: Contributions from Information Systems. *International Review of Law, Computers & Technology*, *17*(1), 85-97.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. BasicBooks.

Liebowitz, S. J., & Margolis, S. E. (1995). Path Dependence, Lock-In, and History. *Journal of Law, Economics, and Organization*, *11*(1), 205-226.

Mill, J. S. (1860). *On Liberty*, Harvard Classics Volume 25, 1909, P.F. Collier & Son. Retrieved January 15, 2008 from http://www.constitution.org/jsm/liberty.htm

McCourt, T., & Burkart, P. (2003). When Creators, Corporations and Consumers Collide: Napster and the Development of On-line Music Distribution. *Media, Culture & Society*, *25*(3), 333-350. DOI: 10.1177/0163443703025003003

McCullagh, D. (2000). Intel Nixes Chip-Tracking ID. *Wired Magazine*. Retrieved January 15, 2008 from http://www.wired.com/politics/law/news/2000/04/35950

Mumford, E. (2000). Socio-technical Design: An Unfulfilled Promise or a Future Opportunity. Proceedings from *IFIP Tc9 Wg9.3 International Conference on Home Oriented informatics and Telematics, IF At Home: Virtual influences on Everyday Life: information, Technology and Society (June 28 - 30, 2000)*. A. Sloane and F. V. Rijn, (Eds.) IFIP Conference Proceedings, vol. 173. Kluwer B.V., Deventer, The Netherlands, 33-46.

Panda, B., Giordano, J., & Kalil, D. (Eds.) (2006). Special Isssue: Next-generation cyber forensics. *Communications of the ACM*, 49(2) ISSN:0001-0782

RIAA, (2007). Retrieved January 15, 2008 from http://www.riaa.com/physicalpiracy.php

Rawls, J. (1999). *A Theory of Justice*. Belknap Press. ISBN: 978-0674000780

Scacchi, W. (2004). Socio-Technical Design. In W.S. Bainbridge (Ed.), *The Encyclopedia of Human-Computer Interaction*, 656-659, Berkshire Publishing Group. Retrieved January 15, 2008 from http://www.ics.uci.edu/%7Ewscacchi/Papers/SE-Encyc/Socio-Technical-Design.pdf

Simons, B. (2000). From the president: to DVD or not to DVD. *Communications of the ACM*, 43(5), 31-32. Retrieved January 15, 2008 from http://doi.acm.org/10.1145/332833.332851

Skovira, R. J. (2003). The social contract revised: obligation and responsibility in the information society. In R. Azari, (Ed.), *Current Security Management & Ethical Issues of information Technology*. Hershey, PA: IGI Publishing. (pp. 165-186).

Stone, B. (2008). Publishers Phase Out Piracy Protection on Audio Books, *The New York Times*. Retrieved May 22, 2008 from http://www.nytimes.com/2008/03/03/business/media/03audiobook.html

Surowiecki, J. (2005). *The Wisdom of Crowds*, Random House Inc.

Torsen, M. (2005). The Domination of the English Language in the Global Village: Efforts to Further Develop the Internet by Populating It with Non-Latin-Based Languages, 12 *RICH. J.L. & TECH. 2*. Retrieved May 21, 2008 from http://law.richmond.edu/jolt/v12i1/article2.pdf.

Thompson, B. (2007). *The obstacles in a DRM-free world*. Retrieved January 15, 2008 from http://news.bbc.co.uk/1/hi/technology/7022157.stm

Wall, D. S., & Williams, M. (2007). Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology & Criminal Justice*, 7(4), 391-415.

Williams, S. (2002). *Free as in Freedom - Richard Stallman's Crusade for Free Software*. O'Reilly. ISBN: 0-596-00287-4. Retrieved January 15, 2008 from http://www.oreilly.com/openbook/freedom/index.html

Whitworth, B. (2006). *Socio-Technical Systems*. Idea Group Inc.

Whitworth, B., & De Moor, A. (2003). Legitimacy by Design: Towards Trusted Socio-Technical Systems. *Behaviour & Information Technology*, *22*(1), 31-51.

Whitworth, B., & Whitworth, E. (2004). Spam and the Social-Technical Gap, *Computer*, *37*(10), 38-45.

KEY TERMS

accountability: the ability to hold a person responsible for their actions, allowing them to be questioned, restrained or punished.

anonymous: namelessness; an agent who is "unnamed/unknown" (that is, an agent who cannot be identified in such a way as to be held accountable); also referring to the creations and acts of creation, of such an agent.

socio-technical systems design: an approach to design that explicitly recognises technology's symbiotic relationship with society, and so tries to involve end-users in the creation of the technical products that will affect their lives.

spoof: to provide false information so as to fool a system and so render it useless.

traceable: the ability to establish a causal link between the source and destination of a communication.

technology creep: the "arms race" that develops in situations where groups having opposing social values try to make use of technology to enforce their views.