
Ethics and Information Technology **3:** 239–246, 2001.

Impersonal interaction and ethics on the World-Wide-Web

David V. Newman
Department of Philosophy, Western Michigan University, Kalamazoo MI 49008, U.S.A. (E-mail: david.newman@wmich.edu)

Abstract. In this paper, I will examine a class of ethical problems that essentially involves computers. I will argue that this class of heretofore unknown ethical problems arise in broadcast communication received with a device of some kind, and involve what I will call impersonal interaction. I also argue that the moral element in such problems lies in a conflict between property rights and free speech rights. Finally, I will argue that the best approach to solving these problems requires the creation of a new standard protocol for computer communication rather than laws governing the use of computers.

Key words: computer ethics, communications ethics, property rights, free speech rights, World Wide Web, WWW

To begin, I want to introduce a situation that I recently encountered while surfing the World Wide Web (WWW), which I will call case A.[1] I had come across references to a researcher whose work might be relevant to my own research, and I found this person's web site through a search engine.[2] While looking over this web site, I clicked on a link that seemed to indicate that the page at the other end would describe the origin of or inspiration for some of the ideas described in the web site. The web page that appeared on my monitor contained advertisements for fee-based pornographic web sites and a suggestive image of a nude woman. Finding this surprise inappropriate and unwelcome, I clicked on the 'back' button in my browser so that I could return to my investigation. A new window opened on the screen, containing another suggestive image and further advertising for one of the fee-based pornographic web sites advertised on the first unwelcome web page. The new window obscured the original browser window. I attempted to close this new window by clicking on the 'close' button. Immediately after the new window closed, a second new window opened containing another suggestive image and further advertising. Closing the second window resulted in a third, and closing the third resulted in a fourth, which finally closed without further difficulty.[3] I was frustrated that my computer had not behaved as I wished and expected it to behave, curious about how this had been accomplished, and disturbed by the level of control that an unknown person had exerted over my computer.

The sequence of events described above is brought about by a combination of events which is common to all use of the WWW. First, a web page author creates a web page and makes it publicly available on a web server. Second, a web page reader uses a computer program called a web browser to request that the page be displayed on his or her computer screen. Third, the web browser program displays the page on the screen of the computer. Fourth, the web browser program monitors the mouse and keyboard of the web page reader for mouse clicks, mouse movements and typed keystrokes (e.g. a keystroke shortcut or command key) to determine what to do next. The third and fourth steps are crucial: in order to display the web page on the reader's computer screen, the web browser program interprets the digital data that the web page author has created as instructions describing what to display, how to display it, and how to respond to subsequent mouse clicks, mouse movements, and keystrokes directed toward the displayed web page. A web page is thus a kind of computer program that in some sense describes its own appearance when viewed using a web browser. Most web pages include only instructions that govern the presentation of text, graphics, or hypertext links (special regions of text or graphics which the web browser software interprets as specifying another web page to be displayed when the web page reader clicks on them with the mouse). For example, Figure 1 illustrates a very simple web page in the form that the web browser software sees it, and Figure 2 illustrates what that page might look like when the browser

[1] Recent news reports by AP and Reuters highlighted similar problems. See http://dailynews.yahoo.com/h/ap/19990923/tc/internet_fraud_3.html.

[2] I do not name the person since I am uncertain who is responsible for the events to follow.

[3] A later visit to confirm the sequence of events was more trying – I closed 17 windows to regain control over my computer. All but two were pornographic in nature.

```
<HTML>
<HEAD>
<TITLE>Example</TITLE>
</HEAD>
<BODY>
<H1>Hello World</H1>
</BODY>
</HTML>
```

Figure 1.

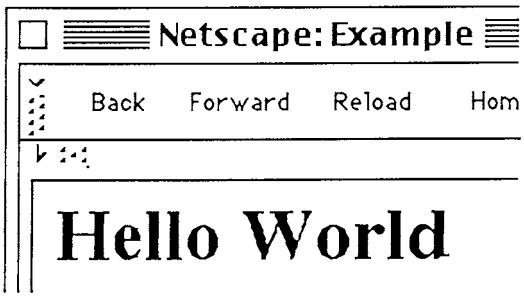

Figure 2.

software has displayed it.[4] The instructions are simple in that they tell the web browser software to use the word 'Example' as the title for the web page, and to display the phrase 'Hello World' as a level-1 headline.

A web page author may also include instructions in a language called *Javascript* in a web page.[5] *Javascript* is a very powerful language, and a web page author who uses *Javascript* can make web pages that are dynamic or that interact with the web page reader in sophisticated ways. The authors of the web pages described in case A included *Javascript* in their pages; that *Javascript* altered the behavior of my web browser software and opened the new windows on my computer screen. Web pages that include *Javascript* and those that do not both operate within the four-step framework described here: web page authoring, web page requesting, web page displaying, and keyboard and mouse monitoring.

Case A and the four-step framework illustrate the features of the WWW that characterize the moral problems I want to examine. First, web pages are a form of broadcast communication. Information is provided on web pages for others to read, and web pages are provided by an author to anyone who requests them in a way that makes them simultaneously available to many individuals.[6] In the particular kind of broadcast communication with which I am concerned, the authors of the communication need not be (and probably are not) actively involved in the broadcast itself. Indeed, the broadcast in case A is completely automated. Second, web pages are different from other forms of broadcast media in that they determine how the artifact used to receive them responds to manipulation of its controls, and the number of possible responses is huge. The artifact required to request and read a web page is a computer with a web browser program. By this mechanism, web pages are immediately responsive to the actions of each reader, and they can change the normal operation of the computer and web browser software. In most cases the immediate responsiveness of a web page consists only in the ability to scroll through the page as necessary, the ability to click on a hypertext link to see another web page, or the ability to interact with other buttons displayed on the web page. However, web pages that include *Javascript* have a more general responsiveness: such pages can respond to the user in many more ways than a page without *Javascript*. The greater number of responses possible using Javascript arises because the interaction can involve multiple steps (a series of interactions) rather than simply a single response to a single user action, and because the response can involve conditional responses that depend on combinations of actions by the user. I will call the first feature impersonality and the second interactivity.

Case A illustrates this impersonal interaction. I viewed web pages provided as a broadcast to anyone on the WWW. I did not choose to visit the second, third, fourth, or fifth web pages in the sequence described above. The web page authors decided that anyone who attempted to use the 'close' or 'back' buttons when viewing these web pages should visit another similar web page. While these actions were responsive to my behaviors in that the actions were performed when I clicked the mouse on the 'close' or

[4] In most web browser software the 'Page Source' menu item in the 'View' menu (or its equivalent) can be used to display the program the web browser software follows to display the web page. The language in which these programs are written is called HTML for Hyper Text Markup Language.

[5] *Javascript* is not normally displayed by web browser software. However, it can often be seen when it is present by using the 'Page Source' menu item in the 'View' menu (or its equivalent). Another language called *VBScript* is roughly equivalent to *Javascript* but it is only found in Microsoft Internet Explorer. The language called *Java* can also be used to create sophisticated web pages, but *Java* programs are not included in the web page in the way that *Javascript* programs are.

[6] Strictly speaking, it is possible for web pages to be used privately rather than as a part of a broadcast media. However, I am concerned only with those web pages used in a broadcast media.

'back' buttons, the web page author had changed the normal effect of these buttons by including *Javascript* instructions in those four web pages. It is my claim that any situation involving impersonal interaction that takes control of a person's computer without informed consent brings about a species of moral problem that is only possible with computers.

Situations in which a user's control over his or her computer is usurped by virtue of the two features described above are morally problematic because they involve a conflict between two fundamental rights. On one hand there is the right to control one's owned property, and on the other hand there is the right to freedom of speech. We can consider each of these in more detail. In the case described above, I was unable to use my computer as I wished. I was prevented from continuing my research in a timely fashion. Windows were created on my computer which I did not intend to create. Perhaps more importantly, the responses of my computer and its software to my manipulation of their controls were changed without my consent. The 'back' and 'close' buttons of the browser windows were changed to open new windows in addition to their normal function. My control of my computer and its software was usurped. There are a number of ways that one can avoid losing control of one's computer in this way. One can turn off certain features in one's web browser software (*Javascript* in this particular case), one can avoid the relevant web sites, or one can reboot the computer or restart the software at the first sign of trouble. However, the fact that I can avoid a situation in which a right of mine will be usurped does not mean that the right does not exist. Moreover, as I will suggest below, there is no practical way for the average user to inspect a web page for unwanted features before viewing it. This means that there is no effective way to have informed consent regarding the activities of the relevant web pages and consequently no effective way to avoid the sites that may violate one's property rights. In addition, I believe there is an expectation that web pages will not change the normal effects of the controls of a web page reader's computer or software. Web pages that do change these features are relatively rare, and it is a principle of good user-interface design to avoid changing the default behavior of the user's computer and software. In addition, prior to the invention of computers, there were no devices that allowed the functions of their controls to change flexibly, invisibly and without any apparent intervention. For these reasons, it cannot be the case that I have given implicit consent to others for this degree of control over my computer.[7] Furthermore, alternative explanations of the wrong done me in this case are implausible. This is not a situation like that described by the phrase *caveat emptor* (buyer beware) since I have no right to purchase goods suitable for my purposes, while I do possess a right to control my property. While Case A may or may not be a kind of harassment, if it is harassment it is not harassment simpliciter because harassment need not involve infringement on one's property rights, which is crucial to the broader class of situations I am trying to characterize. Thus, the actions of the web page authors really do usurp control of my computer and its software, which is a violation of my property rights.

In the case described above, the web page authors were arguably exercising their right to free speech. If this is the case, we should not restrict what the web page authors put on their web pages without good reason. Creating a web page available on the WWW can be viewed as a broadcast of textual, video, or audio information to all users of the WWW. The broadcast is a set of instructions which web browser software can interpret as describing a presentation including text, graphics, audio, and certain interactive features of the web browsing software. It seems clear that the text, graphics and audio are forms of speech even given their historically unusual mode of delivery. The web page as a whole must also be a form of speech since its intention is to provide information to a reader. That the web page is essentially a set of instructions which the audience frequently never sees is not relevant since the same can be said of a musical score, a film script, or a manuscript of a speech. This set of instructions is also analogous to the speech of a person who says 'jump off a cliff' to everyone he or she meets. Such instructions are rude but not immoral unless the listener is unable to protect him- or herself from these instructions; we regard it as the responsibility of normal adults to protect themselves from such harmful instructions, and the state only steps in to protect those who cannot protect themselves. Web page authors are arguably publishing information in a new form that should be afforded the same protections afforded other forms of speech. Even if the speech in question is offensive or objectionable, it is often recognized that offensive or objectionable speech must be protected in order to maintain the freedom of speech for all. One may object that the speech in question is not protected by analogy to our ability to prohibit anyone from yelling 'Fire' in a crowded theater. However, the analogy isn't clear since web sites arguably have more features of traditional publishing than of this kind of prohibited speech: web

[7] I have clearly given implicit consent to the display of textual, graphical, or audio information, and arguably even consent to the execution of well-behaved Javascript programs, but I haven't given consent to programs that usurp my control of my computer or that change its normal behaviors.

sites have extended duration, they are widely distributed, web page viewers must request delivery of a web page, and the harms caused by the web pages are not generally great enough to prevent their publication (see below for further discussion of the potential harms). In addition, since speech that we definitely want to protect can be produced using web pages (for example, political speech), there is a *prima facie* case that web pages should be protected speech. Thus, if we prevent a web page author from publishing a web page including a *Javascript* program that may take control of my computer, there is a case to be made that we are infringing his or her right to free speech.

The conflict of fundamental rights described above is sufficient to make this a moral problem, but there are also real and potential harms that may arise as a consequence of viewing a web page. Some real and potential harms that may come about as a result of visiting a page containing *Javascript* are relatively minor, and they may be so minor as to qualify only as annoyances rather than as morally significant harms. In case A I have been forced to pay for a small amount of electricity that I would not otherwise have used, and I have been forced to take a few minutes of my valuable time to regain control of my computer. Others who accessed this web site using a modem and metered phone service or metered internet access might be forced to pay a slightly greater phone bill or internet service bill than would otherwise be the case. If these harms were present but the violation of property rights was not, then the free speech rights of the web page author would presumably determine our response to the situation. However, there is also the potential for greater harm. Risks Digest reports that under certain circumstances, web page authors can seize more complete control of a web-surfer's computer, potentially deleting files from the hard drive or reading confidential data.[8] It is also possible to create web pages which may force the web page reader to quit and restart his or her web browser (and possibly the computer), and which may crash the web page reader's computer, possibly leading to the loss of data.[9] It is also possible to create web pages containing javascript which, when stored as a bookmark, will disclose data on the web page reader's computer to others.[10] If, as some suspect, computer software cannot be provably secure, hackers of the future may find severe security problems with (future versions of) web browser software that are currently not known. Thus, there are grave potential harms for those who use the WWW. On the other hand, the majority of web speech is not harmful, and the existence of potential harms in web pages are not necessarily a moral problem, particularly if many of them are trivial. I thus conclude that it is the conflict between free speech and property rights that is the essential problem in case A.

The conflict of rights I have described is made slightly more complex when the web page reader is using a computer that he or she does not own. If the web page reader is renting, leasing, or borrowing the computer, or if the web page reader is an agent for the owner of the computer (e.g. an employee of the owner who is using the computer at the direction of the owner), the owner has temporarily transferred some of his or her property rights to the web page reader, and the conflict of rights described above may still arise. Similarly, if the computer is public property, the user's shared ownership of the computer will allow the conflict of rights to arise. However, if the web page reader is an illegitimate user of the computer who has no property rights in the computer, the conflict of rights cannot arise. Two responses are possible here. First, we may say that the fact that the problem does not arise when the web page reader does not have property rights in the computer he or she is using does not show that there is no moral problem in cases where the web page reader does have property rights in the computer. Perhaps a web page reader without property rights in the computer is simply being harassed. Second, we may suggest that because web pages have some sort of implied warranty regarding their fitness or suitability for use, and that web pages that modify the default behavior of a computer are morally wrong on the grounds that they have violated this implied warranty. However, violation of an implied warranty is independent of the conflict of rights described above because it would appear in those cases where property rights were involved as well as those where property rights were not involved. Violation of an implied warranty also does not essentially involve the interactivity of the computer. Thus, these complications do not alter the moral problem involving the conflict of rights though they suggest that the moral problem in question is only present when the web page reader owns the computer he or she is using.

I now want to discuss the reasons why computers are essentially involved. The principal reason is that computers are the only artifacts that are interactive in the way described above. Interactivity, in this sense, requires that an artifact have the ability to change its own normal operations and controls in arbitrary ways. Only computers have this kind of flexibility. This is

[8] Risks Digest 20 #30, Friday 16 April 1999. See http://catless.ncl.ac.uk/Risks/20.30.html.

[9] See http://pbc.bhcom1.com/usenet/Malicious.htm. Technically sophisticated users can sometimes avoid the harmful effects of these web pages.

[10] See http://linuxtoday.com/stories/6211.html.

another way of saying that only computers are general-purpose programmable devices.[11] Other devices may have a limited number of pre-programmed or built-in modes of operation, and may be able to switch between them when external signals are received, but only computers have an infinite number of modes of operation and can interpret external signals as a program describing such a mode of operation.

Interactivity in this sense is not shared by any other kind of artifact or device for the reception of broadcast communications. Televisions and radios are not interactive in the sense described above. While one might say that they respond immediately to channel or frequency changes or perhaps to telephone calls to the transmitting station, they cannot change the operation of the device through which they are received. It isn't possible for a television show to change a television set into a video game machine, or for a radio show to cause one's automobile to drive to an advertised location. Or, if these capabilities were added to televisions or radios in their full generality, televisions and radios would arguably be transformed into computers. Most of the responses described above are not really responses by the artifact since the new broadcast program that one receives after changing the channel or the frequency was already in progress beforehand. A call to the transmitting station may result in immediate changes to the content of the program, but a broadcasting station cannot respond to every member of the audience, and the response is directed by a human being rather than the television or radio in any case. Other media that one would normally consider to be interactive are not impersonal broadcasts, and they aren't interactive in the right sense of the term. Salespeople can block the normal effect of a doorknob by putting their foot in the door, and telephone solicitors can block the normal effect of the phrase 'goodbye' by ignoring it when it is spoken, but neither of these are impersonal, and they do not involve a broadcast to a large audience. Perhaps more importantly, in neither case is there a change of the controls of the artifact in question: the doorknob and the telephone continue to operate in the normal way. Most artifacts cannot interpret and respond to speech in any form, or when they can, it is simply a choice between a limited number of options, as when a voice-sensitive light switch turns itself on or off in response to a spoken command. Computers, however, can interpret speech as a set of commands to be followed without question, and these instructions can be made sophisticated enough that it is difficult to overcome attempts to control them.[12] Thus, it is precisely the most interesting feature of computers – their ability to execute a stored program – that leads to the moral problem described here.

One may suggest in response that this problem is simply another conflict between two fundamental rights that have conflicted before. For example, one may say that this kind of case is similar to other free-speech cases where the speech is unwanted.[13] This case is different from other unwanted speech cases in two ways. First, in the other cases, the speech is unwanted because it is offensive or because it is thought to be harmful to the community via its influence on listeners and their subsequent behavior under the influence of the information contained in the speech. However in this case, neither the offensiveness of the material presented nor the uncertain effects that the speech may have on human listeners plays any part in the moral question. The moral problem lies in the fact that the web page reader's computer is controlled by another person's speech against the will of the computer's owner, and that the computer owner's property rights were thus compromised. Second, other purportedly similar cases do not have the combination of features present in this case. In this case, the problem is interactive and impersonal. In the purportedly similar cases, the unwanted speech is not interactive in that there are no artifacts involved, or if there are, they cannot monitor or respond to the recipients' behavior in the way described above, or if it is interactive, it is not impersonal in that the person making the speech must be present. Thus, the moral problem here is a new one that did not exist before the invention of computers since only computers can provide the kind of impersonal interaction required to generate the problem.

We can compare the case described here to other cases that do not involve computers in order to make the novelty of this case clearer. Door-to-door salesmen reportedly sometimes put their foot in the open door of a home to prevent potential customers from closing the door before the sales pitch is finished. While the salesman takes control of the door and interacts with the potential customer in a way that is infinitely responsive to the potential customer's behavior, the salesman must also be physically present in order to

[11] I have in mind artifacts that implement the Von Neumann or Turing machine models, or artifacts functionally equivalent to them.

[12] Viruses, worms, and trojan horses are extreme examples of programs that attempt to take control of a victim's computer in a way that makes it difficult for the victim to regain complete control of the computer. If they can be interpreted as forms of broadcast speech, they may fit into the category of impersonal interaction as well.

[13] Some examples might include: profane speech, inciting a riot, yelling fire in a crowded theater, telephone solicitation, or false advertising.

do so. Some advertising reportedly includes subliminal messages that exert some control over those who are exposed to it. However, the level of control isn't as great as the control over my computer described in case A, and the message isn't interactive or responsive to the behavior of the viewer or listener. Print advertising or signs exert no control over an artifact and are thus not interactive. Unsolicited advertising sent via FAX machine (which I believe is now illegal in many jurisdictions) exerts some control over the recipient's fax machine, but it is not interactive because the fax machine does not respond to the behavior of the recipient in a flexible way. Finally, weather radios that turn themselves on in response to a weather alert also do not respond flexibly to their owners. This is a small sample of the possible contrasting cases; while I cannot prove that no cases involving impersonal interaction of the kind described here and the conflict between speech and basic freedom existed before computers were invented, I have not been able to think of any such cases, and the nature of the problem suggests to me that only in computers will such cases arise.

The case described above is not the sole case that exhibits impersonal interactivity; other cases exist. Before turning to consideration of possible responses to this problem, I will present three similar cases for comparison. Recall that I have called the case described at that outset Case A. Case B is a case with which I am personally familiar, while the remaining cases are cases I have learned about from news reports.

> **Case B**: When surfing the web, a small window containing advertising sometimes opens on the screen. This window appears most frequently at sites supported by advertising (e.g. any of the free web sites hosted by GeoCities). If this window is closed or if another window is placed on top of this small window, the small window is frequently reopened or placed atop all other windows once again.
>
> **Case C**: Stuffit Expander 5.1 for the Macintosh is a free computer program available for download from many web pages. Every time it runs, it will instruct a Macintosh computer using the Internet Config utility program (installed by default in version 8 and above of the Macintosh operating system) to use Stuffit Expander as the default program for expanding compressed files. The user may explicitly tell Internet Config to use another program as the default program for expanding compressed files, but if Stuffit Expander 5.1 is ever used after this default setting is created, the setting will be changed to use Stuffit Expander. The software does not notify the user of the computer of the change or ask for permission.[14]
>
> **Case D**: QuickTime 3.0 was a free program available for download from Apple Computer's web site. Some versions of the QuickTime 3.0 software by Apple Computer put an icon on the desktop of Macintosh computers every time it was run. This icon advertised QuickTime 3.0 Professional which was not free. If the user deleted the icon, it was restored the next time the software was run. The user was not informed about this before the software was installed.[15]

In each of these cases, a piece of software broadcast via the internet has taken control of a computer used to receive the broadcast and performed actions that the owner or user of the computer may not want the computer to perform. In case C, the computer user may have explicitly indicated that the action in question should not be performed, while in the remaining cases there is no way for the computer user to express a preference either way.

These additional cases share the features of case A: they all involve the broadcast of information to an audience, and each member of the audience uses a computer to receive the broadcast. In each case, the broadcast material is responsive to the user's actions, and the broadcast contains instructions to the recipient's computer which usurp the recipient's control of that computer to some degree. However, there are also differences between the cases. In cases C and D, the instructions are not human-readable as they are in cases A and B. In case C, no advertising is involved, while in the other three cases the motivation for usurping control of the user's computer involves advertising for a commercial product. In case A, the advertised material was potentially offensive due to its content, but this feature is not shared by cases B or D. These differences help to show that the crucial issue is the conflict between the property rights of the web page reader and the free speech rights of the web page author. Because the use of different technical methods could have made the instructions human-readable in cases C and D or not human readable in cases A and B, we can see that the mode of presentation of the speech is not the moral issue. Because most of these examples do not involve potentially offensive content, and because at least one case does not involve advertising, we can see that the content

[14] See http://www.macintouch.com/stuffit5.html#internetconfig. This was later removed from the program due to public pressure.

[15] See http://www.macintouch.com/qt3.html. This was later removed from the program due to public pressure.

of the speech is not the moral issue. Therefore, any response to the problem must focus on resolving the conflict between property rights and free speech that arises when artifacts can bring about situations with impersonal interactivity.

One way to respond would be to find a way for web page readers to protect themselves from infringement of their property rights and from potential harms. Even today some forms of self-protection are available. Those who wish to protect themselves from infringement of their property rights can simply refrain from surfing the WWW, but this is a harm since use of the WWW can be beneficial. Those who can accept more limited protection can turn *Javascript* and similar technologies off, but this is a harm since these features are often beneficial, and in any case this will not protect computer owners from unknown security problems in their web browser software. Those who seek to make informed decisions about what web pages to view can view web pages the first time with *Javascript* and similar features turned off to validate the WWW pages in question, and then turn on *Javascript* selectively later for validated web pages. However, this is impractical because it requires a level of technological sophistication that many do not have or want, and because it takes considerable time and effort to validate and revalidate all the pages that one may want to view. In addition, this approach will not solve the problem since the analysis of *Javascript* programs is potentially difficult and subject to error. Using professional services to examine and rate all web pages is another possible approach to informed consent. However, this would be expensive and inconvenient, and may not solve the problem since even experts may err when analyzing complex web pages. In the absence of other methods of self-protection, social action must be considered.

The problem is a difficult one since the right to control one's personal property and the right to free speech are both regarded as very important. The ideal solution should somehow preserve both of these rights. We should not prohibit the use of computers and web browser software that enables the problem to arise, since this would be to restrict owners' control over their computers in order to protect owners' control over their computers. We should not prohibit the creation of web pages that are interactive since this would be too great an infringement on the free speech rights of web page authors. More sophisticated and discriminating prohibitions are difficult to formulate since the relevant technology is changing rapidly and since the existing problems are probably not well enough understood. Voluntary ratings systems are not practical given the anonymity possible on the WWW and given the probable deception on the part of those who want to cause trouble for web page readers. Legally required rating systems would arguably be contrary to the right to free speech. Therefore, we must somehow find a solution that allows the WWW and similar technologies to continue to exist, while at the same time protecting the property rights and the free speech rights of all parties.

The creators of the *Java* language have attempted to solve this problem technologically by creating a 'sandbox' for Java programs to 'play' in, thus protecting a computer from their activities. However, creating such a form of prophylaxis is a technologically difficult problem, and this approach seems likely to result in an arms race between those who seek to protect property rights and those who seek to violate them (such an arms race is already on to some degree in the area of computer viruses). This approach also requires that such protective software be written for every piece of software that might allow information downloaded from the internet to usurp control of a computer.[16] I thus seek an approach to the problem that is more general and which has fewer technological problems.

Since the problem lies in the interaction of two agents in a computer network, a new communications protocol seems to be the right sort of solution. In many of the cases above, the conflict between the web page reader's right to control his or her computer and the web page author's freedom of speech could be avoided if the web page reader could be better informed about the consequences of reading the relevant web pages. The problem is that the unwanted features of a web page are hidden prior to their activation. Put another way, there is no way for a web page reader to negotiate the conditions under which a web page will be allowed on his or her computer. The web page is either viewed or not, and the web page reader's consent is not informed consent since the relevant features are not disclosed prior to viewing the page. Thus, if the protocol under which web pages are viewed included a method by which the features of the web page were disclosed, this would create informed consent with respect to the activities that the web page would perform on the web page reader's computer. This suggests that a new protocol for the WWW is required, one in which the features of the relevant web page are disclosed before the web page is read. If such a protocol were implemented, a web page reader who

[16] For example, separate solutions are required for *Java*, *Javascript*, *VBScript*, and any other software with the same functionality. In addition, cases C and D show that a solution may be required for the operating system, in order to allow downloaded software to be used. This proposed solution is thus close in spirit to the approach that has been taken to protect computers from virii and other dangerous software.

clicked on a link in a web page might be presented with a dialog indicating that the web page they are about to read contains *Javascript* in addition to standard HTML. If necessary, the dialog could also indicate that the page contains references to *Java* applets, *VBScript*, and other potentially harmful information. This approach would allow web page readers to make more sophisticated decisions about the web pages that they want to view rather than simply turning *Javascript* on or off for all web pages at once. This approach also has the potential to keep pace with advancing technology since it would be easy to expand the disclosure dialog to include new potentially dangerous features of web pages in the future. Moreover, if the protocol is a kind of meta-protocol, then other similar technologies could be subsumed under it as well as the protocols that govern the WWW (http protocol, ftp protocol, and others). Thus, the WWW and other similar technologies should be subsumed by a new computer communication meta-protocol that governs the disclosure of important features of broadcast communications.

There are disadvantages to this kind of protocol. Such a negotiation protocol will introduce a kind of inefficiency in that it will require that computers (and possibly their users) perform an extra step before a web page is viewed. It will require additional network traffic, and thus will consume some network resources. Such a protocol may also demand a level of education for computer users that is perhaps difficult to achieve.[17] Some may argue that such a protocol is a restriction on free speech rights since it prevents certain kinds of surprising speech and certain kinds of civil disobedience via computer.[18] Finally, the hackers of the world will undoubtedly find ways around this new protocol, perhaps through simple deception.

In spite of these disadvantages, I believe that a network disclosure protocol is the right approach to the problem described above. The principal advantage of such an approach is that it recognizes that some cases of impersonal interaction are desirable and some are not. Impersonal interaction is only immoral when the informed consent of the property owner is not obtained ahead of time. The implementation of such a protocol would allow WWW users to control their own level of risk. It may be best to use a combination approach including both disclosure and something like the *Java* sandbox approach. If both these features are present, then computer users will be able to make informed decisions about how much risk they want to undertake, and they will be able to confidently assume that their computer will follow that decision. In addition, if the only way around the protocol is through deception, then the authors of web pages that usurp control of a computer must conceal the fact that the web page will usurp control of the computer in order to convince people to view the web page. If this happens, then the authors of these web pages will be liable for the deception, and hence no law concerning the problem of impersonal interaction will be required. However, due to the complexity of the systems in question and due to the ingenuity of those involved in the computer industry, the problem probably cannot be eliminated completely by institution of a new protocol. For this reason, it seems that we will continue to be faced with this problem, though we may be able to significantly reduce its scope.

Thus, in this paper, I hope to have shown that there is at least one new ethical or moral problem generated by the invention of modern stored-program computers. I hope to have also shown that this problem involves a conflict between the values of personal freedom and free speech. Finally, I hope to have argued that the best response to the problem is a new communications protocol in which broadcast materials would disclose their features before being communicated to a recipient.

[17] I suspect that the protective features of existing web browser programs are not widely known by WWW users. For example, there are methods to prevent one's browser from accepting cookies, from executing *Javascript* scripts, and from executing Java applets; however, many people are ignorant of these methods and thus are unaware of a kind of control that others have over their computers via these mechanisms.

[18] I owe this objection to my colleague Insoo Hyun.