An Introduction to Issues in Computers, Ethics, and Policy

Gordon Hull

* Note: The following text is complete except for chapter 6, “Subjectivity and Sovereignty” and a brief conclusion, both to be inserted. (GH, 8/13/00)*

An Introduction to Issues in Computers, Ethics and Policy

TABLE OF CONTENTS

CHAPTER I: INTRODUCTION

This is a book about "computers, ethics and policy." It is not a book of "computer ethics," and in it, you will not find lists of rules for how ethical people use computers, or formulae for how to decide if a given computing practice is or is not ethical. Rather, by putting an "and" between the terms of the title, I intend to indicate the intersection of several different topics.[1] On the one hand, there is ethics, understood as the philosophical study of how people ought to relate to one another. On the other hand, there is the set of phenomena called by such words as "information technology," the "computer revolution," the "information superhighway," and other such popular buzzwords. The social attempt to deal with these phenomena results in various policies. Any of these topics can be studied on its own. However, studying them together presents a number of difficult and troubling questions. This is a book about some of the questions which emerge when one tries to think about both computers and ethics together, and when one then tries to establish policies and institutions that reflect this thinking.

In this sense, it is a book more about "critical thinking" than it is a book of "applied ethics," assuming that applied ethics is the enterprise of adapting general principles of ethical theory to specialized situations – business, medicine, and so forth. It can and should be extended to the study of computers and computing technology. However, without passing judgment on the viability of applied ethics in general, it seems that one should note that many of the ethical problems which emerge with computer technology do not seem to fit traditional ethical categories very well. Indeed, some of the most difficult problems emerge precisely when our ethical theories do not seem to fit developments in technology and its general diffusion. This is the space for critical thinking: for developing the resources to think about ethics, and to make educated, informed decisions about what to do. Critical thinking is a process and not a result; developing skills in critical thinking is not a matter of the memorization of tables or formula. It is a matter of continual effort and practice. Additionally, because many of the situations presented to us by computer technology do not have precise analogues in the physical, "bricks and mortar" world of traditional ethical theory, it will be very difficult to know for sure what the "right thing to do" is. In such cases, the best we can hope for is to have as many people as possible who are capable of thinking carefully about the issues at hand.[2]

Technology and Society: The Scope of the Topic

Unless you have been hiding under a rock for some time, you will have heard that computers are important and that their widespread use has implications for all of society. Lots of people offer fantastic sounding propositions about how wonderful or how bad our world will be as a result of computer technology. Bill Joy, the founder of Sun Microsystems, surprised many with his dystopic predictions in the April, 2000 issue of *Wired* magazine. The surprise in Joy's case was not that he predicted that technology would cause problems. It was – as he took considerable effort to point out – that he is himself one of the "insiders," one of the creators of the computer society. After detailing some apocalyptic scenarios involving genetic engineering gone awry and uncontrollable "nanotechnology," he suggests that:

[1] I owe the conjunctive phrase "computers and ethics" (rather than "computer ethics") to Professor Stephen R. Schach, whose "computers and ethics" course I TA'd. The "and policy" reflects my sense of the pressing urgent reality of the topic.

[2] The study of computer ethics does not require or presuppose an extensive familiarity with computer technology. One needs to know *what* people can do with computers, but it is less important (in most cases) to know *how*.

> The question is, indeed, Which is to be master? Will we survive our technologies? We are being propelled into this new century with no plan, no control, no brakes. Have we already gone too far down the path to alter course? I don't believe so, but we aren't trying yet, and the last chance to assert control – the fail-safe point – is rapidly approaching.[3]

Pronouncements such as Joy's offer at least two occasions for critical thought. First, of course, is the implicit ethical challenge: Joy thinks that the human species as a whole lacks the ethical values to handle the technology it is creating, and that the survival of humanity depends on rapidly developing those values. Second, and this is the point that is more striking at the moment, one needs the critical skills to evaluate such apocalyptic claims. Both apocalyptic and utopian claims about computers and technology are very easy to find. Neither is of any help at all unless they can be read critically; claims such as "there will never again be any moment in life with privacy" are not very helpful unless one can know how and why they might be true.[4] More than with many other topics, the world of computer technology is, after all, a *human* creation, which means that very little about it is a matter of pre-ordained necessity. It is rather a matter of addressing the social issues brought on by this human creation.[5]

Whether or not one believes that computer ethics is a topic of universal proportions, it is an important topic. Money is not the only thing of value in the world, but the presence of a large amount of it some place generally is a good sign that people think that place is important. In this regard, some economic figures might help to indicate just how important people think computer and information technology is and is going to be. As with all printed statistics about the computer industry, these will be dated by the time you read them. But they should at least give a sense of the scale of the issues involved.

According to a June, 2000 Department of Commerce report, "Americans have definitively crossed into a new era of economic and social experience bound up in digitally-based technological changes that are producing new ways of working, new means and manners of communicating, new goods and services, and new forms of community."[6] By 1997, the United States was spending roughly

---

[3] Bill Joy, "Why the future doesn't need us," *Wired* (April 2000), at URL: http://www.wired.com/wired/archive/8.04/joy_pr.html.

[4] One commentator suggests that "for the mainstream media, the Net is most easily characterized as the source of new threats to the individual, even though many of these new threats are merely old threats cloaked by new technology." Mike Godwin, "Net to Worry," *Communications of the ACM* 42:12 (December 1999), 16.

[5] This point is emphasized particularly in Lawrence Lessig, *Code and other Laws of Cyberspace* (New York: Basic Books, 1999). One should also underscore that the "market" within which computer technology operates is also a human creation, and operates by means of and through the structures (legal and otherwise) in which products are bought and sold. On this point, see also James Boyle, *Shamans, Software and Spleens* (Cambridge, Mass: Harvard UP, 1996), 89 ("there *is* no 'natural,' unregulated state of affairs. Without the rules of contract, tort, and property there would not *be* a market"); and Sam Pooley, "The State Rules, OK? The Continuing Political Economy of Nation-States," *Review of Radical Political Economics* 22:1 (1990), 45-58. This point will be implicit in what follows; I will discuss issues of sovereignty in the final chapter.

[6] United States Department of Commerce, *Digital Economy 2000*, at URL: http://www.esa.doc.gov/de2k.htm. See also the summary in "Super Economy," *PC Magazine* (June 13, 2000), at URL: http://www.zdnet.com/pcmag/stories/trends/0,7607,2587342,00.html.

$643 billion annually on information and communication technologies. As of that same year, information technology (IT) industries accounted for an estimated 7.8 percent (7.8%) of U.S. GDP and 12.4% of its nominal growth, while for 1998 the preliminary comparable figures were 8.2% and 14.7%.[7] These statistics tell us two things: first, that information and communication technologies occupy a growing percentage of the U.S. economy; and second, that the rate at which that percentage is growing is itself growing. Similarly, in 1995, IT's share of all research and development spending in the U.S. was 43.7% and rising, and by 2000, business spending on information technology equipment should exceed half of all spending on capital equipment.[8] In 1998, IT spending accounted for a third of all company-funded research and development.[9] None of these numbers include industries, such as biotechnology, which depend heavily on developments in computer technologies (the genome project, after all, was sequenced by computer).

In terms of personal use, between 1996 and 1998, Internet utilization grew from forty (40) to 100 million people. In 1998, forecasters speculated that usage of the Internet would increase to 320 million people by 2002, when Internet use for commerce between businesses alone might amount to $300 billion.[10] According to the Department of Commerce Report, global Internet access rose from 171 million to 304 million people between March 1999 and March 2000 alone, an increase of 78%.[11] Furthermore, the long-held United States dominance in Internet use is eroding: during this period, Internet usage in the U.S. and Canada increased 41%, but in all other regions of the world, it more than doubled, causing U.S. and Canadian use to now (for the first time) reflect less than half the total. The Web is now estimated to contain over 1 billion unique pages.[12] It should be underscored how recent much of this is: the Internet did not exist as a commercial entity until the mid-1990's. The original Department of Defense network which became the Internet began operation only in 1969, and with only four nodes.[13] This rate of diffusion vastly exceeds that of any previous major technology.

Despite this exponential growth, the diffusion of computer technologies remains staggeringly uneven, and not just in terms of the so-called "digital divide" in the United States. Although African Internet usage increased 136% in the last year, there were still only 2.6 million people online in the entire continent as of March, 2000. In the "Asia-Pacific" region, only 68.9 million people had Internet access (most of them in Japan).[14] Yet there are over one billion people in the People's Republic of China alone. As one commentator put it:

---

[7] The following statistics are taken from: John M. Conley, *et. al.*, "Database Protection in a Digital World," Richmond Journal of Law and Technology 6:2 (Symposium 1999), at URL: http://www.richmond.edu/jolt/v6i1/conley.html

[8] *Ibid.*

[9] Department of Commerce, *Digital Economy 2000*.

[10] John M. Conley, *et. al.*, "Database Protection."

[11] Department of Commerce, *Digital Economy 2000*.

[12] *Ibid*. The difference between 1998 and 2000 numbers should suggest the rapid increase in the rate of increasing Internet usage: if global Net usage increases 78% again in each of 2000 and 2001, the correct usage number for 2002 will be 963 million, over *triple* the original projection. That one can alter projections so easily also suggests that the projections should be read for the general message they convey, rather than any precise statistics.

[13] For a brief history, see Peter J. Denning, "The Internet after Thirty Years," in Peter J. Denning and Dorothy E. Denning, eds., *Internet Besieged: Countering Cyberspace Scofflaws* (New York: ACM Press, 1998), 15-28.

[14] Department of Commerce, *Digital Economy 2000*.

> The map of the globe at the end of the twentieth century is not of a planet blanketed by a reassuring web of communications and transportation technology-the global is not planetary in any sense of the word. Whole continents are spanned or bypassed by the supposed global Internet, as are entire regions within countries and within cities. This map of the globe is notable for its lumpiness, its unevenness, and its extremely bifurcated and patchy distribution of resources both within countries and between countries, on every level, from the local to the international. How and why these sharply differentiated spaces came into being are pressing questions.[15]

This exponential and uneven growth in the usage of computers poses ethical, legal, and political questions which not only do not have easy answers, but which require some sort of immediate policy. The Internet can be used for a wide range of activities, from lawn and garden chat rooms to viewing pornography to freely copying music. All of these are in some way different than they were before. Copying music, for example, no longer requires the physical presence of a record or CD bearing it. Rather, the music can be copied into a file, and then sent anywhere in the world. This in turn creates pressure on a legal system that was designed to deal with print media and other forms of communication that depended on the information being inseparably linked to the object carrying it, be that object a book, a CD, or whatever. The prospect of the sudden growth of "disembodied information," in other words, is one of the defining characteristics of the computer age, and one of those with which our traditional ways of thinking are, apparently, not prepared to cope.[16]

The widespread and rapid emergence of computer technology has also created debates among and about those who operate and program computers. As computer programming becomes less the pastime of garage "hackers" and more a large-scale business, it faces many of the questions which face other professions. Are computer programmers or software engineers "professionals," in the same sense that doctors and lawyers are? If so, should they be governed by a special code of conduct? Should they be licensed like doctors and lawyers? However one answers these questions, it remains that as society becomes increasingly dependent on computers and information technology, those who are able to control and operate this technology will be an increasingly powerful segment of society, and questions about the social responsibilities that go with such power will be unavoidable.

The contemporary importance of this question is underlined in two ways. First, according to a study released in Spring, 2000, there will be 1.6 million jobs available in the information technology sector in the U.S. in 2000. Of these, almost half will remain unfilled because of a shortage of qualified workers.[17] This shortage has in turn led to pressure on Congress to increase the number of skilled-worker Visas allowed into the United States.

---

[15] Keith Aoki, "Considering Multiple and Overlapping Sovereignties: Liberalism, Libertarianism, National Sovereignty, 'Global' Intellectual Property, and the Internet," *Independent Journal of Global Legal Studies* 5 (Spring 1998), 456.

[16] For a historical study of the development of "information" from ancient societies to its contemporary near absolute separation from the algorithms which manipulate and create it, see Michael E. Hobart and Zachary S. Schiffman, *Information Ages: Literacy, Numeracy, and the Computer Revolution* (Baltimore: Johns Hopkins UP, 1998).

[17] NPR, Kaiser Family Foundation and Harvard University, *Computer Use Survey* (February 2000), at URL: http://www.npr.org/programs/specials/poll/technology/index.html

However, this leads to objections on two fronts. On the one hand, the Immigration and Naturalization Service, the government branch responsible for processing these visas, is *already* so overloaded that, although many visas are requested, many fewer than the maximum are actually granted any given year. On the other hand, labor groups object that importing foreign workers to fill skilled jobs in the United States disenfranchises large numbers of American workers by denying them the skills training needed both for their own welfare and for long-term American economic competitiveness. Other countries, in particular Germany, are also increasing their quotas for specialist workers: the shortage is global. In sum, there is a pressing need for skilled computer workers, and this need is so great that the demand for workers itself generates difficult social and ethical questions.

Second, the Association for Computing Machinery (ACM) and IEEE have now adopted a software engineering code of ethics. This adoption was not without controversy, and the ACM takes the strong position that *licensing* software engineers is a bad idea. One should also note the difficulty in separating the ethical question from the political ones: if there were a licensing requirement for software engineers, how would it work, since there is such a shortage of software engineers? The preamble to the ACM code is instructive, because it indicates a professional awareness of the growing importance that those who understand how to operate computers do so responsibly:

> Computers have a central and growing role in commerce, industry, government, medicine, education, entertainment, and society at large. Software engineers are those who contribute by direct participation or by teaching, to the analysis, specification, design, development, certification, maintenance, and testing of software systems. Because of their roles in developing software systems, software engineers have significant opportunities to do good or cause harm, to enable others to do good or cause harm, or to influence others to do good or cause harm. To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession. In accordance with that commitment, software engineers shall adhere to the following Code of Ethics and Professional Practice.[18]

Finally, since "ethics" is, after all, also a part of philosophy, it is worth noting the extent to which computing is beginning to give rise to philosophical questions. In one sense, these questions have been around for along time, in particular questions about the extent to which artificial intelligence programs could or could not ever be sufficiently sophisticated to count as "minds." This debate, which becomes surprisingly complicated very quickly, however, has begun to expand. For example, how should one understand "hypertext," the dominant point-and-click format of WebPages, where one can instantly be transformed not just to a different location at the same site, but to a site in another part of the world? What does this mean for our understanding of literacy and reading? The questions can also be practical: how can and should (these are separate questions) computers be used in education in subjects in the humanities? Computers apparently do an excellent job teaching formal logic – but can they teach writing? Do we want them to? What about

[18] Don Gotterbarn, Keith Miller and Simon Rogerson, "Software Engineering Code of Ethics is Approved," *Communications of the ACM* 42:10 (October 1999), 102-107.

online universities? Do they spread education to everyone, finally dethroning the "ivory tower" of the academy, or do they offer corporations a cheap way to train people as workers while depriving those people of any sort of real education as citizens and thinkers (in short: as people)?[19] The following passage is perhaps hyperbolic, but it is from the preface to a recent book on "How Computers are Changing Philosophy:"

> Computing provides philosophy with such a set of simple, but incredibly fertile notions – new and evolving *subject matters, methods,* and *models* for philosophical inquiry. Computing brings new opportunities and challenges to traditional philosophical activities. As a result, computing is changing the professional activities of philosophers, including how they do research, how they cooperate with each other, and how they teach their courses. Most importantly, computing is changing the way philosophers understand foundational concepts in philosophy, such as mind, consciousness, experience, reasoning, knowledge, truth, ethics and creativity. This trend in philosophical inquiry that incorporates computing in terms of a subject matter, a method, or a model has been gaining momentum steadily. A Digital Phoenix is rising![20]

In other words, the awareness of the importance of computing extends not just to professions and people immediately involved with computers, but to all sections of society.

The complexity of the social and ethical questions surrounding computer technology requires underscoring in at least one other important way. Americans are inclined to think that life divides neatly into "government," on the one hand, and the people, business, markets, etc. on the other. Political philosophy then becomes about how to protect the second group from the former. In its more extreme forms, this becomes a form of "libertarianism," which says that government is always on the way to being a "Big Brother" which takes away the freedom of its people. This form of political philosophy is particularly prevalent among those who think about computers, many of whom believe that one consequence of the Internet will be the inability of government to maintain its power over people. Certainly among the most famous of such announcements is Electronic Freedom Forum founder and Grateful Dead lyricist John Perry Barlow's "Declaration of the Independence of Cyberspace," which declares (in part):

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the

---

[19] For the two sides in this debate, see "US billionaire to launch free cyber university," *The Times (London)* (March 16, 2000); and "Commentary: E-Education, the opposite of equality," *Los Angeles Times* (March 23, 2000).

[20] Terrell Ward Bynum and James H. Moor, "How Computers are Changing Philosophy," in Terrell Ward Bynum and James H. Moor, eds., *The Digital Phoenix: How Computers are Changing Philosophy* (Oxford: Blackwell, 1998), 1.

> tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.[21]

As he indicates, Barlow wrote this in response to the proposed 1996 Telecommunications act; many of the parts of the law to which he was objecting were struck down by the Supreme Court.[22]

Taken to an extreme form as a philosophy of computing and society (as opposed to as a manifesto or call to arms), this does a disservice to its adherents, because it is completely blind to the complexity with which our society and legislative process operate. At the very least, and as a start, it should be noted that it is often corporate lobbying that gets restrictive laws passed, over the initial reluctance of lawmakers. The current copyright laws, for example, are largely the result of heavy lobbying by the entertainment industry. When the Walt Disney Corporation wanted to buy the distribution and marketing rights for the "classic" Winnie the Pooh, the corporation made the purchase contingent on passage of an extension to how long works like Pooh could be copyrighted. Seeing the profit-potential of Pooh and the possible loss of Mickey Mouse as a source of profit (because Mickey Mouse was old enough to be near the freely copyable "public domain," Disney chairman Michael Eisner personally lobbied Senate majority leader Trent Lott and gave campaign contributions to ten of the original thirteen sponsors of the legislation that came to be known as the "Sonny Bono Copyright Term Extension Act."[23] As a result, whether or not it is physically possible to stop people from passing around photos of Pooh, it *is* possible to stop them from marketing books that use the Pooh characters, and it is *illegal* to copy those photos.

In short, "the market" is not separate from the government and the individuals, and *often it is corporations and the industry which pressure for big government.* Other times, the government intervenes *against* large corporations, *for the sake of the market.* In this regard, one need only mention the federal government's lawsuit against Microsoft, charging the company's practices with unfairly distorting the computer operating system and software markets. Sometimes, government tries to stop what people do on the Internet, even though that activity might make money, as for example when Congress passes laws against child pornography. Other times, the government tries to encourage use of the Internet through programs to expand and fund access in schools. All of these distinctions can be made without distinguishing between kinds of companies and locations of government. In other words, the questions of government, markets, and individuals are complicated and changing in form.

The foregoing has, I hope, indicated some of the complexity and a few of the issues surrounding the intersection of computers and ethics, considered as part of the intersection of computers and people. In this book, I hope to lead a topical exploration of some of those issues.

Ethics, Law, Policy, and Politics

A survey of the various topics in this book might bring one to an immediate question: why, if this is a book about "ethics," is there so much about law (for example, copyright law), politics

---

[21] John Perry Barlow, "A Declaration of the Independence of Cyberspace" (1996) at URL: http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration

[22] See the crime chapter, below, on "Pornography."

[23] Jon M. Garon, "Media and Monopoly in the Information Age: Slowing the Convergence at the Marketplace of Ideas," *Cardozo Arts and Entertainment Journal* 17 (1999), 523-524, and 523 n. 152.

(national sovereignty), and public policy (privacy laws)? This is an easy question to answer, but the second part of the answer may seem contentious.

First, the topics included here are traditional in discussions of computer ethics. For example, in her groundbreaking textbook *Computer Ethics*, Deborah Johnson included chapters on professional ethics, privacy, crime, and copyright law.[24] One of the most commonly cited articles which makes a strong ethical claim about using computers is Eugene Spafford's "Are Computer Break-in's Ethical."[25] However, when one reads the article, it could equally be described as an article about "crime:" Spafford is describing a kind of hacking that is generally against federal law.

Second, and this is the contentious part, it seems difficult to draw sharp lines between "ethics" and "politics," at least when one is talking about using computers. In its modern forms, "ethics" is generally defined as the study of how one person should relate to another. For example, it is normally considered wrong to lie to someone. But sometimes the context in which the question is asked seems to make a difference. To take a famous example, suppose that the people in question are a doctor and patient, and the patient has just been diagnosed with a terminal illness. To what extent should the doctor tell the patient immediately and directly? How about the patient's family? What if the patient is a child? At the end of the day, the doctor might still have an obligation to tell the patient the "whole truth and nothing but the truth." But the context seems to make the question rather more difficult. To take another example closer to the context of computers: suppose that "I" am a fictitious character existing "in cyberspace," a personality existing separately from my "real," embodied self. What if my fictitious character wants to injure somebody else's fictitious character? Where do "my" obligations lie – or, more to the point, "whose" obligations are they? Finally, suppose that I do not know exactly what the effects of my action will be, or who exactly they will affect? Suppose that my actions will "decrease consumer confidence in the technological stock market." How does one evaluate that?

These are not idle speculations. "Multi-user domains" (MUD's) refer to cyberspace locations where people can develop Internet personae, which then interact with one another. One's Internet character can be very different from one's "real" character: a tall, fat, man can become a short, thin woman, and no one will know. In one such MUD, called "LamdaMOO," where was a character called "Bungle" who had the "voodoo" power to take over other characters and make them appear to do things they were not actually doing. One day, Bungle took over the voices of a number of women characters, and violently raped them, while making them seem to enjoy the rape.[26] I do not wish to settle a discussion here about "what" happened. I simply wish to point out that one reason we say rape is wrong is that it seriously hurts a real person. What Bungle did may be equally wrong – but to say that will require settling a number of questions about who Bungle is, and who the women he attacked are. Admittedly, the Bungle case is particularly striking in its strangeness. But there are other equally difficult examples, and those examples often stretch our habitual ethical categories substantially.

A philosophical purist may respond that this is may or may not be idle, but that it is not philosophy. To this I can only respond: it is the field of questions that people using computer technology

[24] Deborah G. Johnson, *Computer Ethics* (Upper Saddle River, NJ: Prentice Hall, 1994).

[25] Eugene Spafford, "Are Computer Hacker Break-ins Ethical?" in *Internet Besieged*, 493-506.

[26] See Julian Dibble, "A Rape in Cyberspace," *Village Voice* (December 23, 1993), at URL: http://www.levity.com/julian/bungle_vv.html, and the discussion in Lawrence Lessig, *Code and Other Laws of Cyberspace*, 74-75.

give us. If that field of questions is no longer the field of "ethics," then so be it: it seems better to study the questions than debate about the right name to give them. For most people, however, I suspect that the case of Bungle will seem very much like an ethical question. If our ethical categories are not ready to tackle it, then we will have to expand our categories.

One place where a lot of "ethical" thinking about computer technology has been taking place is law. This is perhaps the product of necessity. Hackers do not wait for our ethical categories to include them before breaking into systems, and corporations do not wait for philosophy to descend from the ivory tower with a thorough understanding of "private property" before taking legal action against those whom they think are stealing from them – as, for example, by freely swapping copyrighted music on the Internet. For reasons such as this, much of the discussion in this book will be about topics which can be included in questions of law and public policy. These fields provide a very rich set of reflections on how people can and should use computer technology, as well as an endless set of difficult examples.

What, then, is "Computer Ethics"

As should be evident, I favor adoption of a broad, inclusive, and fairly imprecise definition of "computer ethics" as the set of topics which emerge at the (changing and multiple) intersections of computer and information technologies and the various components of society. In particular, I do not think that the "ethics" component can be easily separated from questions of "politics," "law," and the like. While such a definition has neither the advantage of precision nor that of great conceptual rigor, it seems to be among the only definitions broad enough not to risk immediate obsolescence, on the one hand, and abstruse irrelevance, on the other. This notion of an intersection between computers and people is a minimum common denominator of most efforts at academic definition of the term. For example, the term "computer ethics" was coined by Walter Maner in the mid-1970's "to refer to *that field of applied professional ethics dealing with ethical problems aggravated, transformed or created by computer technology*."[27] As his usage of the word "applied" suggests, Maner was primarily concerned with linking traditional ethical theories (see Chapter II) with computer technology. The proliferation of developments in computer technology has stretched the possibility of this application considerably.

In her *Computer Ethics*, Deborah G. Johnson argues that computer ethics be understood as a set of "new species of old moral issues."[28] One can note that this is a logical extension of Maner's general point. Such definitions carry within themselves a remarkable tension. On the one hand, by attaching computer issues to traditional ethical questions, they focus the debate on application of those ethical theories and suggest that ethical theory should have philosophical priority over technological practice. On the other hand, in bringing together computers and traditional philosophy, these definitions suggest that this priority should be questioned. After all, there is no *a priori* reason to believe that our "old moral issues" can adequately deal with questions posed by the usage of computer technology. Of course, there is no reason to believe that they cannot, either, but the question does not seem to be one that should be closed in advance. The available evidence does seem to

---

[27] Qt. in Terrell Ward Bynum, "Global Information Ethics and the Computer Revolution," *The Digital Phoenix*, 277. The restriction to applied professional ethics, for example, also occurs in Donald Gotterbarn: computer ethics is "a branch of *professional ethics*, which is concerned primarily with standards of practice and codes of conduct of computing professionals" (qt. in Bynum, 281). While I agree that professional ethics is a relevant question to ask of a computer ethics, it seems entirely too restrictive to limit the term in that way.

[28] Deborah G. Johnson, *Computer Ethics*, 2nd ed. (New Jersey: Prentice Hall, 1994), 10.

suggest that the fit will be difficult. James H. Moor, in his prize-winning article of 1985, offers a more inclusive definition:

> "On my view, *computer ethics* is the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such policy." (266) "The mark of a basic problem in computer ethics is one in which technology is *essentially* involved and there is an uncertainty about what to do and even about how to understand the situation" (267), hence "computer ethics is a dynamic and complex field of study which considers the relationships among facts, conceptualizations, policies and values with regard to constantly changing computer technology." (266)[29]

This definition seems sufficiently broad, and highlights a few important issues. First, as the preceding discussion has indicated is important, the definition is both inclusive and flexible. Second, it is policy oriented. This is one way to understand the sense in which computer ethics is "applied:" if it is to matter to real people, then it will necessarily involve issues of public policy. Finally, Moor focuses on the technology and its importance.

The focus on the technology is perhaps the final reason why computer ethics needs to be understood broadly: computers themselves are extremely flexible machines. As Moor puts it, "what is revolutionary about computers is *logical malleability*. Computers are logically malleable in that they can be shaped and molded to do any activity that can be characterized in terms of inputs, outputs, and connecting logical operations …. The computer is the nearest thing we have to a universal tool."[30] I do not wish to engage in the difficult questions of the logical specification of what a computer is. It should suffice to here to indicate that modern digital computers are generally instantiations of Turing machines, which means that they are algorithmic: they can do anything which can be specified in terms of Boolean logic.[31] Many people argue that this includes all things that humans can do; others extend this to the idea that the universe itself is algorithmic.[32] Regardless of how far one wishes to extend this understanding of a computer, the point about logical malleability is an important one and should be retained. Because a computer can do anything which can be put in algorithmic form, and because this includes operations on "data," its power to create and manipulate the external world is without precedent. Algorithms themselves can be viewed as data and vice versa. Hobart and Schiffman suggest:

---

[29] James H. Moor. "What is Computer Ethics?" *Metaphilosophy* 16:4 (October 1985), 266-275. I have rearranged the order of Moor's presentation; page numbers are cited inside the passage.

[30] James H. Moor, "What is Computer Ethics," 269.

[31] To this should be added the caveat that new developments in computer technology may ultimately surpass the limitation on Boolean and binary logic. In particular, quantum computing holds out this possibility. See, for example, Neil Gershenfeld and Isaac L. Chuang, "Quantum Computing with Molecules," *Scientific American* (June 1998), at URL: http://www.sciam.com/1998/0698issue/0698gershenfeld.html.

[32] The former suggestion has spawned a lengthy and bitter debate in philosophy, dating back to questions about whether artificial intelligence programs could ever constitute a "mind." The latter suggestion (about nature itself) seems extravagant. For a development of it, see Jon Barwise and John Etchemendy, "Digital Metaphysics," in Terrell Ward Bynum and James H. Moor, eds., *The Digital Phoenix: How Computers are Changing Philosophy* (Oxford: Blackwell, 1998), 117-134.

> Logic binds digital data; it is the set of rules according to which the data symbols may be moved. Once in 'motion' data comprise algorithms. And each step in an algorithm must be unambiguous and rigorous, logically necessary, following without exception from its predecessor to which it is chained by the rules. The steps of this movement comprise our information age's internal 'chains of reason,' its central power. Only through its exercise can there emerge the patterned strings of 1s and 0s by whose means we can encode the 'stuff' of our exchanges with the world. At the deepest level, then, the logical, algorithmic power of computer technology actually constitutes information.[33]

In its broadest sense, computer ethics is about what happens in the space of human relations when such technology is a part of the world in which people live.

A note on Argument

If the field of computers and ethics is a complex and difficult one, we should not expect it to reduce easily to formulae. This means that there will perhaps be fewer easy and certain answers than one would like, and many more seemingly intractable problems. Furthermore, if the boundaries between ethics and politics cannot be sharply drawn in the case of computing, then some of the messier aspects of the political process are going to be unavoidable. Even worse, sometimes the conclusions one draws depend entirely on which of two (or more) very important values one says is *more* important. For example, if free speech is absolutely important, then *no* form of copyright law makes any sense. On the other hand, if property rights are absolutely important, then it makes perfect sense to require that always people pay before using ideas created by others. Debates about copyright (and other forms of intellectual property) and computers even tend to polarize into two camps such as these: those who think that (for example) software should be free, and those who think that copying of software should be both heavily restricted and heavily penalized. What is one to do? Claiming that the other side is "biased" doesn't help very much, since the other side could make the same claim that about you and be just as correct – as far as they're concerned.

If, at the end of the day, ethics is about what people should do in a given situation, then it requires that we develop the ability to make judgments, and to be able to say that "this course of action is right, and that course of action is wrong." Of course, put in such simple terms, this might or might not help very much, since different people are likely to have different understandings of right and wrong, as the example of free speech versus copyright should suggest. Philosophers have tended to try (as we shall see in chapter 2) to sort out standards for right and wrong that would apply to any situation or to all people. Even if one assumes that such a procedure is possible, there is still the matter of applying those standards to less abstract situations and to real people. Sometimes, it appears that choices about what one "should" do cannot be easily placed into the category of right and wrong. Speed limits provide a good example: most people can agree that residential streets should have a speed limit in order to promote public safety. Whether that speed limit should be 30mph or 35mph, however, is something which ought to be able to be decided, but as a decision, it lacks a lot of the urgency of most questions of "right" and "wrong." Nevertheless, setting one speed limit and not another is an essential step to having a speed limit, as much as the initial decision to regulate speed. One prominent scholar put the issue clearly: "we must recall that both ethics and public policies often entail not a choice between good

[33] Hobart and Schiffman, *Information Ages*, 225.

and evil and right and wrong, but rather the much more daunting challenge of charting a course when faced with two conflicting rights or goods."[34]

In order to be able to meet these sorts of challenges, one needs to be able to make arguments in favor of or against certain choices: "this course of action is wrong;" "that decision is better than this one." Philosophers have studied argument for thousands of years, and have developed some extremely complicated theories to understand them. For the purposes of this text, I prefer a rather simple standard: an argument consists of a claim and a warrant. A claim is what one wants others to believe. A warrant is a reason why they should believe it.[35] Hence, "it will rain tomorrow" is a claim. "It will rain tomorrow because there is an eastward moving cold front west of here," adds the warrant. This definition is minimal, but it does offer some basic points:

- A lot of the work in ethics and policy-making is about evaluating different arguments, and deciding which ones are more persuasive, *i.e.*, which ones are "better."
- Warrants can be of varying types. A lot of the work in evaluating arguments rests in deciding how to evaluate warrants.
- Evaluating arguments can be context dependent: "It is going to rain tomorrow" is an easier point to prove in a tropical rain forest than in a desert.
- A reference to an authority is not necessarily the best warrant. On the other hand, it can be persuasive: "It is going to rain tomorrow because the weather person said so" may not be logically valid, but it can be believable (if it weren't, local news programs would have very little to talk about).
- "I think" is not an argument. "I think it is going to rain tomorrow" is not a better reason to bring out an umbrella than "it is going to rain tomorrow."

In an environment where argument is understood in this way or a similar way, one can separate reasoning and argument from rhetoric (tools of persuasion) only to a certain extent. If arguments are about persuasion, then the most persuasive argument may be the one which is best stated. This has a positive and a negative consequence. On the positive side, it means that crafting one's arguments carefully, and thinking about what kind of argument will be persuasive to what kind of audience, are important points in thinking about ethics. On the negative side, it means that one has to be very careful to sort out *why* one is being asked to believe something, and to evaluate it accordingly. A few moments of reflection on advertising should serve to make this point very clear.

---

[34] Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 1999), 4.

[35] This "sociological" understanding of argument has its origin in Stephen Toulmin, *The Uses of Argument* (Cambridge: Cambridge UP, 1958).

CHAPTER II: PHILOSOPHICAL ETHICS

A complete treatment of philosophical ethics is well beyond the scope of this (or any other) book. Still, it is important to have a basic grasp of the way ethics debates are most often presented. Before dealing with the specific problems of computers and ethics, then, a detour into ethical theory is in order. Two limitations of the scope of this detour should be emphasized. First, the ethical theories considered here are limited to those developed in "modern" philosophy. "Modern" philosophy names a specific historical development in European philosophy dating to the 1600's. Modern philosophy distinguishes itself from ancient and medieval philosophy before it in several ways. These include an effort to separate philosophical from religious thought, and (in ethics) an effort to evaluate morality in terms of individual acts. Ancient and medieval philosophy, in contrast, tended to subordinate human reason to revealed religion and to view morality in terms of a person's overall virtue, understood as a habit of doing the right thing, measurable only at the end of his or her life.[1] Second, the following will consider only "mainstream," "analytic" approaches to ethics. This limitation is primarily imposed by the literature about computer ethics, which tends to take this approach. However, as will be evident in other chapters, many scholars (particularly those working in law) reject many aspects of the analytic ethical tradition.[2] In short, what follows is a very brief introduction to a very rich body of thought, and is intended to be introductory rather than comprehensive.

Foundations

A central feature of most modern schools of philosophical ethics is the presence of a foundation or an "intrinsic good." Indeed, the urge to establish a foundation upon which subsequent thinking could be based was one of the driving motives behind the development of modern philosophy in general. There were many reasons for this urge, but one aspect of most versions of it was a drive for an increased stability and certainty of knowledge. René Descartes, one of the most important early modern philosophers, conveys something of the stakes in this general search for foundations:

> There is not usually so much perfection in works composed of several parts and produced by various different craftsmen as in the works of one man. Thus we see that buildings undertaken and completed by a single architect are usually more attractive and better planned than those which several have tried to patch up by adapting old walls built for different purposes …. Regarding the opinions to which I had hitherto given credence, I

[1] In what follows I will leave aside efforts to develop a modern appropriation of this 'virtue ethics.' See generally the work of Alasdair MacIntyre, *After Virtue: A Study in Moral Theory* (Notre Dame, IN: U. of Notre Dame Press, 1984).

[2] For an exemplary instance of someone who remains committed to analytic ethics but would reject many of the assumptions detailed below, see Luciano Floridi, "Information Ethics: On the Philosophical Foundation of Computer Ethics," at URL: http://www.wolfson.ox.ac.uk/~floridi/ie.htm. I will also leave aside, for the moment, "postmodern" thought, in all its variations. The references to Friedrich Nietzsche, whose words have been instrumental in the development of "postmodernism," are intended to be reminders of this omission. Probably the most important "postmodern" thinker for issues of computer policy is Michel Foucault, who will be discussed explicitly in Chapter 4 (Privacy). Foucauldian concerns are also visible in discussions of intellectual property; see the discussion and notes in Chapter 3 for references.

> thought that I could not do better than to undertake to get rid of them, all at one go, in order to replace them afterwards with better ones, or with the same ones once I had squared them with the standards of reason.[3]

Two parts of Descartes' passage should be emphasized. First, the architecture metaphor suggests that a more pleasing, functional urban system is one which is built according to the same plan and sets of rules. One thinks in this regard of the ease in navigating cities, such as Chicago or Washington, DC, which are built according to a "grid," and the difficulty of navigating cities, such as London, which are not. By analogy, Descartes's suggestion is that a philosophical system would be better if it were built as a whole, from the same set of foundational principles. Second, the point is not necessarily to replace all of one's opinions – the point is to examine those opinions, and make sure that one only adheres to rational ones. Opinions from other sources, such as superstition, the contents of old and poorly remembered books, and custom in general, are to be eliminated. In this way, people will come to realize their potential as rational beings.

Another aspect of Descartes' position which should be noted is its emphasis on an individual person, taken as an autonomous individual, as the primary locus of thought and action. With this emphasis, Descartes contributes importantly to the development of the "subject" as the primary agent of political and ethical activity.[4] Subjects are assumed to be autonomous – capable of free choice – and equal to one another when considered ethically or legally, as such autonomous agents. Something like this understanding of subjectivity lies beneath most of the ethical thought discussed in this chapter. Subjectivity is also one of the concepts which is challenged directly by developments in information technology – a point to which we shall return in the final chapter.

There is a lot built into Descartes' general program, and many objections could be made. The point to underline here is that this sort of a search for foundations, coupled with a usage of the individual subject in a foundational role, underlies both of the primary schools of modern philosophical ethics. As the architectural analogy suggests, one's choice of foundation will have far-reaching effects throughout the system, so the choice of foundation is an important one. Since ethics is about doing good things, and since the best kind of philosophical system (according to this theory) is the one that is universally true, it follows that the best kind of foundation would be the one that describes something which is a good thing for all people at all times – it would be correct for all subjects and subject positions. This "intrinsic good" is something which is good in itself, and does not require justification by other things. Instead, the intrinsic good is the justification for why those other things are good. These other goods can then be called "instrumental goods," because they can be viewed as tools for promoting the intrinsic good. For example, if I believe that getting a good night's sleep is an intrinsic good, then instrumental goods which would help me reach that good might include living in a quiet place, avoiding coffee right before bed, and so forth. Note that one can also debate the relative merits of instrumental goods, as for

---

[3] *Discourse on the Method*, in *The Philosophical Writings of Descartes*, trans. John Cottingham, Robert Stoothoff and Dugald Murdoch (Cambridge: Cambridge UP, 1985), I: 116-117.

[4] For a history of the development of subjectivity, emphasizing its appearance in its modern form as both philosophical and juridical, see Étienne Balibar, "*Sujet, individu, citoyen. Qu'est-ce que 'l'homme' au XVIIe siècle?*" In *L'individu dans la théorie politique et dans la pratique*, ed. Janet Coleman (Paris: PUF, 1996), 249-277.

example, whether or not ethics books, because of the dryness of their subject matter, are good bedtime reading.

The example of getting a good night's sleep shows the difficulty in formulating one's intrinsic good, since there are many people for whom this is not the highest, or even one of the higher, goods. Of course, those people might be wrong, and their being wrong should not matter to my ethical theory, since my theory is about what they *should* do. I do, however, have to be able to produce a reason why they ought to value sleep more than (say) late night television. Not only that, even for those who value their rest highly, there are many occasions where there might be something better: cramming for a test might be the better thing to do *this* night, even if in principle sleep is good. One can imagine many other exceptions and qualifications. At this point, however, sleep no longer sounds like much of a foundation for one's ethical system. It certainly lacks the aesthetic elegance that Descartes seems to imagine would attach to his single-architect city. As it turns out, it is rather difficult to name something which is sufficiently universal that all people either do or should value it as their highest, intrinsic good.

One question which will not seem adequately answered at this point might be: why does one need such a foundation? Sure, modern philosophers have tended to think that foundations are necessary, but why should they be trusted? In ethics debates, the opposing school of thought is often called "relativism," a name which suggests that the answer to the question, "what is the highest good," is relative to the person asking the question. Debates in philosophical ethics tend to posit an initial choice between foundationalism and relativism: *either* one has a universal foundation, *or* one is an irrational relativist.[5] Implicit in this is a value judgment which enables a certain style of argument: the judgment is that almost anything is better than relativism, which means that if I can successfully call someone's ethical position "relativism," I have *ipso facto* refuted it. Accusations of relativism, then, will turn out to be relatively frequent in ethical debates, because they imply accusations of irrationality.

Such accusations are often premature, and an important skill in reading articles about ethics is the ability to discern which of these accusations have any credibility, and which are polemical caricatures of arguments designed to stigmatize them into submission. That said, the problems with relativism are easy to demonstrate, since nobody really wants to live in a world where "anything goes." Suppose that I am an axe murderer, and that I think the best thing in the world for me to do is to chop people into small bits. In a world of true relativism, no one would have any resource for saying that what I did was wrong. I could always respond that although it is perhaps wrong for you, axe murdering is right for me. At that point, the discussion would be over, since neither of us could appeal to a higher authority to justify our actions or to condemn those that we did not like. The world would very quickly become one where "might makes right," and the values and whims of whoever has the most power would be the "correct ones." Not only would such a world probably be unpleasant to live in – or to imagine as the way people "ought" to behave – it does not even really give one a reason to think about ethics in the first place, since ethics implies some sort of standard for what "ought" to be done.[6]

---

[5] Deborah G. Johnson, for example, in her *Computer Ethics*, 2nd ed. (New Jersey: Prentice Hall, 1994), 19-22, strongly implies such an "either/or."

[6] Avoidance of such a "state of nature," in which life would be "nasty, brutish and short," was the motive behind the political philosophy of Descartes' contemporary, Thomas Hobbes, who was the first modern exponent of "social contract theory." Hobbes's point is that human beings need some sort of laws and standards governing them, because to imagine humans in a state absolutely without governance would be to imagine them in the worst of all possible states. The "nasty, brutish and short line" is

There have been two primary foundations in modern ethical thought, consequences and human worth (or human dignity). They have given rise to substantial and competing bodies of literature, and will be examined here in turn. The first school of thought emphasizes the consequences of an act, and the second the act's intrinsic moral worth. Members of the first school tend to accuse those of the latter of irrationality, whereas members of the second school tend to accuse the first of immorality.

First Foundation: Consequences

This school of thought holds that the worth of an action – the place where one looks to decide if it is a morally worthy act – is to be found in its consequences. In other words, any act which has good consequences can be said to be a good act. The obvious question to answer is: what counts as a good consequence. The answer has to be something that would be acceptable to all people, all the time. Most such "consequentialists" have settled upon happiness as their intrinsic good. A good action, then, is one that promotes (human) happiness. However, one can ask an immediate question: whose happiness should the act promote? Again, there have been two primary answers: the happiness of the person who is performing the act, and the happiness of people in general.

When elevated to a school of thought, the first response is generally called "egoism," ("I-ism," for the Latin impaired), and adopts as a principle that the morally worthy act is the one that makes me, the actor, happy. This certainly has an appealing ring to it. On the other hand, few philosophers take it seriously, because it can be made to sound like relativism with very little effort: suppose that what makes me happy is being an axe murderer? If the standard for the morally worthy act is one that makes me happy, then my pleasure at chopping people up with an axe is definitionally morally worthy, and it is hard to explain how it could be otherwise. One could respond that I am deluded about what makes me happy ("the axe murderer is really lonely and miserable") or that I ought to enjoy other things more ("see, it's much more fun to share!"), but at the point one adopts these positions, one is left with very little of the "ego" in "egoism." After all, the whole point had been to found ethics personal happiness; if that happiness immediately has to be qualified by reference to some external standard (what is abstractly good, what would make other happy), then would it not have been better simply to start with the external standard? After all, one's foundation is not supposed to rest on something else.

The second response, that one should look to the overall happiness created by the act, has become the school of thought labeled "utilitarianism." According to a utilitarian, the answer to the question, "is it morally right to do something?" is provided by calculating the net effects of that act, in terms of whether the overall happiness of the world will be increased. Of course, things are not that easy, but before noting complications of the theory, I should note two of its immediately attractive aspects. On the one hand, utilitarianism offers a decision calculus, whereby it is possible to rationally calculate the moral worth of an act. At least in principle, this means that utilitarianism can function as a viable foundation or plan upon which an entire, internally consistent ethical code can be built. On the other hand, utilitarianism has an intuitive appeal, in that it sounds very much like the way that most of us think, most of the time. Economic cost-benefit analysis, for example, is the sort of thing that sounds very much like a utilitarian calculus. As a school of thought, indeed, utilitarianism developed at about the same time as industrialization, and two of its main, initial advocates, Jeremy Bentham and John Stuart Mill, were prominent reformers in mid-nineteenth century England.

The difficulties with utilitarianism begin when one tries to decide how to calculate whether an act produces overall happiness or not. Bentham envisioned something rather like a balance or

---

from Hobbes's *Leviathan* (in any number of contemporary editions), chapter 13.

ledger sheet, on which one could list the pleasure and pain produced by a given act, and then tally the results. A net positive result would be a morally worthy act, and a net negative would be condemned. This manner of thinking is now generally called "act utilitarianism," because it focuses on the individual act itself. There have been many objections to act utilitarianism since Bentham's suggestion of it, and a complete discussion of those objections and their answers could fill a library shelf. For the purposes of this text, I wish to focus on a few, which will serve as exemplary. They are (a) act utilitarianism violates our moral intuitions; (b) it makes supererogatory acts morally obligatory; and (c) the decision calculus is impossible. Let us look at each of these in turn.

The first objection, that act utilitarianism violates our moral intuitions, is very commonly made, and has been made in the context of computer ethics. For example, in his frequently quoted "Are Computer Hacker Break-ins Ethical?" Eugene Spafford condemns act utilitarianism on the grounds that it would legitimate executing smokers. Spafford suggests as an "extreme example" that "the government orders a hundred cigarette smokers, chosen at random, to be beheaded on live national television."[7] He points out that the result would be that *many* people would be deterred from starting to smoke, and *many* others would quit cold turkey. All of those people would likely live longer, more productive lives than if they had smoked. So too, the country would save the costs associated with the treatment of the respiratory diseases that many of them would develop, freeing health care resources to treat other diseases. It therefore seems quite possible to arrive at the conclusion, on act utilitarian grounds, that the unhappiness to the hundred people beheaded would be vastly outweighed by the increased happiness to the hundreds of thousands who would not die of lung cancer. Still, almost everyone would consider such an act deeply wrong, even if they could not say exactly why. Examples of utilitarian calculations generating such troubling results are easy to generate: suppose the slavery of a few would make the majority much happier by increasing their leisure?[8] In its most vulgar form, the objection can be made as follows: suppose that, in a group of 100 people, 51 of them decided they could become blissfully happy by killing the other 49? The easy availability of examples such as this lead many to reject utilitarianism on principle.

This is a standard objection, and it withstands many of the obvious answers: for example, though the hundred people beheaded would presumably be very, very unhappy, there would, after all, only be a hundred lives lost, which seems (from a point of view other than those hundred) like a small sacrifice for the health and lives of hundreds of thousands. Military planners make such calculations all the time. Still, the objection is rather easily countered, not so much because of what it says about utilitarianism, but for what it assumes about our intuitions. The basic problem is that the objection is question-begging, which is to say that it only works as an adequate refutation of utilitarianism if you *already* think that our moral intuitions should have priority over "rational," utilitarian calculations. The objection, in other words, is an example of deontologists calling utilitarians immoral. The utilitarian will answer: the whole point of having a rationalized moral theory like utilitarianism is to discover which of our intuitions we should keep and which we should get rid of. He or she will then continue: the fact that we find something "intuitively" right or wrong does not make it so. Slavery, for example, used to be intuitively acceptable, and so did the notion that women and people of color were naturally inferior to white men. The objection that utility conflicts with intuitions, then, simply establishes that the two

[7] Eugene Spafford, "Are Computer Hacker Break-ins Ethical?" in Peter J. Denning and Dorothy E. Denning, eds., *Internet Besieged: Countering Cyberspace Scofflaws* (New York: ACM Press, 1998), 495.

[8] This example is adduced by Deborah G. Johnson. See *Computer Ethics*, 27-28.

schools of thought can generate contradictory results. What it does *not* show is which result is correct. In order to refute the utilitarian calculus, our moral intuitions would themselves have to be justified, lest they turn out to be like the intuitive justifications of slavery, sexism, and racism. At this point, however, the two camps are back to square one: what is one trying to achieve with a moral theory? In sum, this objection establishes what lawyers like to call a *prima facie* case, which is to say it establishes the possibility that utilitarianism is wrong.[9] It underlines the conflict at the level of foundations: what is the intrinsic good? How does one decide which intrinsic good is better? Does utilitarianism have the resources to avoid such extreme consequences?

A second general objection made to act utilitarianism is that it would make supererogatory (exceptionally praiseworthy) acts morally necessary. This objection derives not from measuring utilitarianism against another moral standard (intuitions), but from attempting to indict the logic of utilitarianism itself. If, according to the act utilitarian, the morally correct act is the one that promotes the most overall happiness, then this would seem to imply that in order to act morally, it is always necessary to try to achieve the most possible good in the world. A moral person would never waste resources on a vacation, for example – he or she would use them to alleviate the suffering of the poor. To be moral at all would require being saintly. In other words, given that one almost always *could* do more to make the world a better place, it is hard for the act utilitarian to explain when one has done *enough*, or has done enough for a reasonable person. This seems to have two consequences. On the one hand, it raises general questions about the viability of the theory as one applies it to everyday activity, since all acts become charged with the obligation to be better. No decision, be it to walk down the street or to take a nap, becomes freed from what becomes an obsessive urge to *do better*. Regardless of whether the world would be a better place as a result of this, it seems not to square with the way people really are. On the other hand, having eliminated the distinction between an adequate and a saintly act, one becomes unable to praise an act as exceptional. The heroic firefighter, for example, who sacrifices his own life to save a family from a burning building becomes not an example of tremendous self-sacrifice, but an example of someone simply doing as he ought. Not only that, but everyone else who saw the fire and did not themselves go rushing in becomes morally suspect.

A third general objection to act utilitarianism is that the decision calculus is impossible, both in theory and in practice. In practice, one is supposed to act in the manner which promotes the most overall good. Each act can be so evaluated, which implies that one should, in each case, decide whether or not what one does promotes the overall good. This seems like a tremendous computational burden to assign. Before doing anything, one is supposed to draw up a chart of utilities and disutilities which might result, and then aggregate them into some sort of composite evaluation of the act. All of this is supposed to happen before doing any act whose moral relevance is being considered, even if the decision to do something has to happen quickly. The firefighter in the previous paragraph, for example, presumably does not have time to calculate the density of smoke in the building and hence the risk of asphyxiation before deciding either to attempt the rescue or not. Act utilitarianism, then, sounds like a better ethical code for computers than for people.

The difficulty is theoretical as well, which is to say that not only are there questions about whether or not a real person could execute the necessary calculations in real time, there are questions about whether or not those calculations could be made at all, in principle. For example, how does one understand the *consequences* of one's act? How do I know what my act will achieve? If the decision is whether or not I should bludgeon someone to death, the consequence is presumably rather easy to discover. On the other

[9] This is not intended to be a technical definition of *prima facie*.

hand, suppose the decision is about whether or not I should drive very fast down a narrow, curved road. At that point, I have to calculate a number of statistical chances that I will lose control of the car, that a deer will jump in front of me, etc. What about long term consequences? Driving a SUV might or might not be gratifying, but insofar as they consume almost twice as much fuel as a car, their widespread adoption might contribute significantly to global warming. How does one understand the effects of global warming? Is global warming really happening? If my driving an SUV causes global warming, and if global warming causes human extinction, then presumably I should stop driving an SUV. What if driving an SUV increases fuel prices? After all, it does increase the demand for fuel, which suggests that the widespread use of SUV's is incompatible with low fuel prices. That SUV's remain so popular suggests the difficulty most people have at attempting such calculations.

A legal version of this problem occurs in liability laws. If I knowingly make a particular product which, say, causes lung cancer when used properly, then I can be held accountable in court for damages which occur as a consequence of my making and advertising that product. This is why cigarette companies have attempted to deny that they knew their products were carcinogenic or addictive. On the other hand, intentionality may or may not be necessary to determine liability: suits brought against gun companies assert that the companies could reasonably know that their products were going to be misused, and should therefore have taken steps to prevent that misuse. The issue is salient to computers because, among other things, many people are considering whether or not companies should be liable for damages to third parties caused by a lack of security on their own systems. Suppose a portal or host site with inadequate security is victimized by hackers, and companies "downstream" lose business. Is the portal site liable for those losses as a consequence of inadequate site security?[10]

To return to utilitarian theory proper, although he is objecting to a specific version of utilitarianism, J. L. Mackie's list of the reasons why calculation is impossible seems generally applicable, and I quote it at length:

> Shortage of time and energy will in general preclude such calculations. Even if time and energy is available, the relevant information commonly is not. An agent's judgment on particular issues is liable to be distorted by his [*sic*]own interests and special affections. Even if he were intellectually able to determine the right choice, weakness of will would be likely to impair his putting of it into effect. Even decisions that are right in themselves and actions based on them are liable to be misused as precedents, so that they will encourage and seem to legitimate wrong actions that are superficially similar to them. And, human nature being what it is, a practical working morality must not be too demanding: it is worse than useless to set standards

[10] See "Directors at legal risk from rise in cyber-crime," *Financial Times (London)* (July 17, 2000), 2; and the analysis in Hal R. Vasian, "Liability for Net Vandalism should rest with those that can best manage the risk," *New York Times* (June 1, 2000), C2. For a critical review of such systems of liability, see Michael Lee, *et. al*., "Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal," *Berkeley Technology Law Journal* 14 (Spring, 1998), 839-886.

> so high that there is no real chance that actions will even approximate to them.[11]

In short, the objection is that there is no possible way to objectively know all the possible consequences of my act. I would have to be God to possess such knowledge.

Partly in response to such objections, utilitarianism has developed a second major strand, "rule utilitarianism." According to rule utilitarianism, the original utilitarian thinkers, particularly John Stuart Mill, should not be read not as having said that each decision one makes should be subject to a utilitarian calculus. Rather, they were suggesting that we as a society should strive for social institutions and practices which, on balance, would increase overall utility. The job of an individual is to follow the rules and practices which have already been justified. Rule utilitarianism, then, combines both a utilitarian calculation with a more traditional conception of rule-following.[12] According to J. O. Urmson, one of the original proponents of this theory, there are four main points to be made: (a) a morally right action is in agreement with a moral rule and a wrong one transgresses a moral rule; (b) a correct moral rule is one which promotes the intrinsic good; (c) moral rules therefore only apply when the general welfare is significantly affected; and (d) when no moral rule is applicable, the act is not evaluated as right or wrong, but according to some other standard.[13]

As a general program, rule utilitarianism seems immediately to relieve many of the difficulties which beset act utilitarianism. Individuals are relieved of the necessity of making difficult decisions in short time spaces: although decisions are difficult, they can at least be made in the relative leisure of policy-making. So too, there no longer seems to be the need for individuals to elevate themselves to the status of saints. Many actions do not significantly affect the overall welfare, and so are not properly evaluated as moral or immoral. On the other hand, many of the same objections seem to be able to be raised. That calculations can be made over a longer period of time does not help if they cannot be made at all, for example. Also, both act and rule utilitarianism are subject to the objection that they reduce humans to vehicles for pleasure. Is not the whole point of being human that one is able to act according to a "higher purpose?" Utilitarianism, however, makes it actively impossible to measure such higher purposes, except insofar as they make people happy. As the philosopher Friedrich Nietzsche sarcastically put it, "insofar as they [utilitarians] are boring one cannot think highly enough of their utility."[14] Animals, after all, seem to be capable of gratification, but one does not necessarily

---

[11] J. L. Mackie, "Rights, Utility, and Universalization," in *Rights and Utility*, ed. R. G. Frey (Minneapolis: University of Minnesota Press, 1984), 91.

[12] This is undoubtedly a legitimate reading of Mill; answering the objection that "there is not time, previous to action, for calculating and weighing the effects of any line of conduct on the general happiness," Mill says that "there has been ample time, namely, the whole past duration of the human species. During that time mankind have been learning by experience the tendencies of actions; on which experience all the prudence as well as all the morality of life are dependent." He adds, in a comment that should be remembered when reading contemporary discussions of ethics, "there is no difficulty in proving any ethical standard whatever to work ill if we suppose universal idiocy to be conjoined with it." J. S. Mill, *Utilitarianism* (Indianapolis, IN: Hackett, 1979), 23.

[13] See J. O. Urmson, "The Interpretation of the Moral Philosophy of J. S. Mill," in *Contemporary Utilitarianism*, ed. Michael Bayles (New York: Anchor Books, 1968), 17. *Contemporary Utilitarianism* anthologizes a number of the important articles which debate the relative merits of rule utilitarianism as a theory.

[14] Friedrich Nietzsche, *Beyond Good and Evil* §228, in *Basic Writings of Nietzsche*, trans. Walter Kaufmann (New York: The Modern Library, 1966), 347.

want to reduce human life to that. Mill places the burden for answering this objection on culture, which will tends towards the development of a sense of "virtue" in individuals. Hence, Mill speaks of a "cultivated mind," by which he means:

> Any mind to which the fountains of knowledge have been opened … finds inexhaustible interest in all that surrounds it: the objects of nature, the achievements of art, the imaginations of poetry, the incidents of history, the ways of mankind, past and present, and their prospects for the future …. There is absolutely no reason in the nature of things why an amount of mental culture sufficient to given an intelligent interest in these objects of contemplation should not be the inheritance of every one born in a civilized country. [15]

So: attending the opera is more worthy than, say, watching professional wrestling, and "it is better to be a human being dissatisfied than a pig satisfied; better to be Socrates dissatisfied than a fool satisfied."[16] Even with such an account, however, it both seems difficult to provide an objective criterion to determine what makes a pleasure more or less worthwhile, and to justify this account in terms of what *actually* makes people happy. After all, opera makes many people perfectly miserable, and professional wrestling makes many more people blissfully happy; distinguishing between them on the grounds that opera *should* make people happy seems suspect in a theory which is supposedly grounded on the maximization of happiness.[17]

A variation of utilitarianism which is worth highlighting in this context goes under the general name of "risk analysis," since it is a way of thinking essential to policy-making, economics, and how most of us lead our daily lives. In general, the idea is that one tries to evaluate a consequence as a function of the likelihood it will happen, as weighed against how good or bad it is. Something very likely and somewhat bad is to be preferred, perhaps, over something which is unlikely but worse. For example, one might ask: "is Internet shopping worth the risk?" One then decides not just what the risks are – credit card theft, loss of privacy, etc. – but how bad those risks are. For example, one faces almost a certain loss of privacy. Perhaps one does not value this sort of privacy very much. Perhaps one is shopping for pornography, and Internet shopping seems *more* private. These examples suggest a general point. Risk analysis, however one actually sets up the calculation, can be a useful exercise for critical thinking, not only because it helps one to evaluate consequences, but because it forces one to be clear about what those consequences are, both in terms of their likelihood and severity. This is important, because in the real world, almost nothing is (100%) "safe" or (100%) "unsafe." Rather, safety and risk are relative terms, which have to be evaluated "on balance" or "on the whole."

A rough way to think about risk is as a multiplication of the percentage chance that something is going to happen, together with its severity or weight. To use a vulgar example, a 50% chance that 100 people will die can be seen as an equivalent risk to a 100%

[15] J. S. Mill, *Utilitarianism*, 13-14. See also his discussion of the development in his Chapter IV, 34-38, and of the "higher faculties:" "It is an unquestionable fact that those who equally acquainted with and equally capable of appreciating and enjoying both do give a most marked preference to the manner of existence which employs their higher faculties" (9).

[16] J. S. Mill, *Utilitarianism*, 10.

[17] Hence, Mill postpones the question to one of progress and moral development.

chance that 50 people will die. This example will also show the limitations of risk analysis: the notion that one is actually calculating is more useful as a heuristic than an actual device, and many of the so-called calculations have to be approximations based on very imperfect evidence. Finally, note the real difficulty faced by a general who faces a scenario like the above. How does one evaluate human life? Should one reduce human life to a calculation? What does one do when there are no easy alternatives – when *neither* action seems particularly desirable?

Risk analysis also raises important questions when one thinks of things which are very unlikely but catastrophic, or nearly inevitable but minimally bad. In other words, is a "systemic" impact worse than a "one shot" one? A few examples will perhaps serve to clarify. During the first part of the Clinton administration, following a series of foreign-policy mishaps, many commentators suggested that these mishaps should best be understood as part of a pattern of incoherent foreign policy. Although one could look for the specific reasons why, for example, the Somalia intervention failed, it would be better to point to a systemic problem, that "this administration would not recognize a foreign policy principle, phony or otherwise, if it tripped over one in the street."[18] The results of such systemic incoherence added up to something more than the aggregation of a series of Somalias. Another example in the same vein is global warming: scientists generally agree that global warming will be seen through its effects, but that these effects will occur, for example, in changed weather patterns. Tropical storms will become more frequent, monsoonal cycles may change, and so forth. These sorts of systemic impacts are hard to measure against, for example, the risk that country x may fight a war against country y, but one often has to think about their relative importance.

On the other side of the coin, one has to think about the extent to which it is rational to avoid very unlikely, but potentially catastrophic impacts. In other words, all other things being equal, should one weigh more heavily the likelihood or the cost of an even occurring? Global nuclear war is a classic example: the possible consequence would be planetary extinction, so one might conclude that it is a consequence to be avoided *at all costs*, meaning that *no* action which could be shown to risk leading to such a global nuclear war should be sanctioned, *no matter how unlikely* the result seems. Other examples come from decisions about environmental risks. As Kristin Shrader-Frechette puts it, "in certain cases, risk consequences are more important than the accident probabilities. For one thing, greater social disruption arises from one massive accident than from a number of single fatality accidents, even the same number of people may be killed." She then uses the example of Russian roulette: "suppose the probability that a bullet is in a chamber when the trigger is pulled is 1 in 17,000 – the same likelihood, per reactor-year, as a nuclear core melt … A person could still be rational in her refusal to play the game …. She could even maintain that the probability in question is irrelevant. Any probability of fatality might be too high if the benefits … were not great enough."[19]

These examples may seem distant from the topic of computer ethics, but similar calculations occur there. For example, given that computer technology enables individuals and groups to encrypt their data sufficiently securely that it could never be read without the key, should there be a requirement that keys be stored in a safe place where government can access them, in order to be able to read the information obtained after a warrant and search? This has been one of the most violently contested questions in U.S. computer policy, and we will return to it in the chapter on privacy.

---

[18] Charles Krauthammer, "Capitulation in Korea," *The Washington Post* (January 7, 1994), A19. Clinton's foreign policy marks rose steadily since.

[19] Kristin Shrader-Frechette, *Risk and Rationality* (Berkeley: U. California Press, 1991), 94-95.

For now, notice the relevance of risk to some solutions: one commentator suggests that "although many of the dangers are hypothetical (for instance, a terrorist holding a nuclear bomb, threatening a city), the disutility of any such dangers is so high that greater attention to public safety seems justified."[20]

Second Foundation: Human Dignity

This school of thought is often called "deontology," and stands for the principle that an act is good or bad independently of its consequences. In other words, the consequences are irrelevant to its moral worth, no matter how good or bad those consequences may seem to be. Rather, one is to focus on the worth or dignity of those who act. This way of thinking has recently been put with particular clarity by Alan Gewirth.[21] Gewirth cites the example of those who threatened Martin Luther King, Jr. with responsibility for any rioting by white supremacists following his speeches. After all, since the rioting would not have happened absent King's speeches, the argument goes, and since the rioting was bad, King should not have given (and should not give more) speeches. In response, Gewirth suggests what he calls the "principle of the intervening action," according to which one notes that it was the white supremacists who chose to riot, not King. Since one should only be responsible for what one does, there is no way to hold King culpable for the actions of white supremacists, and that a morality which does is flawed. Gewirth's reason why is given in another example, which extends the principle as far as it can go. Suppose that a group of terrorists possess a nuclear bomb, and threatens to use it to blow up New York City, unless someone publicly tortures his mother to death. In this case, even though millions of people might die "as a result" of his refusing to torture his mother, he is nonetheless fully justified in the refusal: one is morally responsible for one's own actions, and it is absolutely morally wrong to torture an innocent person to death, even though the case presents "a tragic conflict of rights and an illustration of the heavy price exacted by moral absolutism."[22]

Gewirth's examples make clear at least two points about deontology. First, and again, deontology focuses narrowly on the responsibilities and duties of a given actor in determining whether or not what he or she does is morally worthy. Second, these responsibilities and duties are oriented around a regard for other people as people. The first philosopher to rigorously formulate this way of thinking was Immanuel Kant.[23] Although Kant wrote before the utilitarians, his theory in many ways seems almost designed to take their theories head-on. The precise content of Kant's argument is both complicated and a subject of debate; for our purposes here, the following reconstruction will suffice.

(1) For morality to be a form of knowledge worthy of the name, it must be universal, like reason and mathematics. To understand this, it is perhaps worth remembering that Kant was a classic enlightenment thinker, which means that "reason" for him is

---

[20] Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 1999), 185.

[21] The following are taken from Alan Gewirth, "Are There Any Absolute Rights?" in his *Human Rights: Essays on Justification and Applications* (Chicago and London: University of Chicago Press, 1982), 218-233. I am reversing the order of Gewirth's examples for narrative effect.

[22] "Are There Any Absolute Rights," 226. Gewirth does have his concrete absolutist offer some further rationalizations based on the principle of intervening action: the certainty of one's mother's death when one tortures her oneself is greater than the certainty either of the terrorists actually launching the nuclear devise or their being appeased by the death of the mother.

[23] The succinct version of the original is in Kant's *Foundations of the Metaphyiscs of Morals*, available in a variety of contemporary editions, for example trans. Lewis White Beck (New York: MacMillan, 1990). Kant's doctrine is explained further in his *Critique of Practical Reason*, trans. Mary Gregor (Cambrdige: Cambridge UP, 1997).

something which is both a good thing and always the same. Since other sciences aim at such knowledge – and mathematics is a paradigmatic case for Kant – there is no reason for morality to settle for less. Otherwise, morality would simply be a study of what customs people have, without the capability of critically reflecting on those customs to see if they are worth having.

(2) If morality is not universal, it won't take account of what makes humans special. Although humans might not act like it, they have at least the potential of being rational agents. This is unlike any other species, and it is what it means to be human. Indeed, morality as a human capacity at all is predicated on human freedom, which means the human ability to make decisions based on reason, and not on sensuous impulses and pleasures. This proposition will perhaps sound suspicious to the contemporary reader. Kant's general point can also be put negatively: if we do not view human rationality as a special feature of humans, then we reduce ourselves to animals.

(3) Pleasures and happiness are (a) always subjective and (b) not unique to humans. You will already recognize this as a form of objections to utilitarianism. What makes *me* happy might or might not make *you* happy, and what makes people in contemporary society happy might not have made the Romans happy. If this is true, however, then even though it may be true that all humans desire pleasure and it is universal in that sense, pleasure is not universal in the relevant sense, because it does not mean the same thing to all people. Furthermore, animals seem to experience pleasure, which means that a morality based on pleasure would tend to reduce humans to animals.[24]

(4) One must look at the act itself – but morality, because it's rational, is about the *reasons why* you act – it is the *principle* that matters. This distinction is absolutely essential, and is commonly not understood.[25] The analogy with mathematics is perhaps again instructive: the Pythagorean theorem is able to do the work it does because it can be expressed in a formula, which means that it can tell you how to make a right triangle. In this sense, it is useful in a way that several pictures of triangles lined up together is not.

(5) The principle involved must be rational, or it's less than human. This principle is called the "categorical imperative:" a moral act is one done both in accordance with and out of respect for the moral law. Kant offers two important versions of it: (a) act so you could will the principle of your action to be a universal law without contradiction,[26] and (b) never treat people merely as a means, but also as ends in themselves.[27] Kant illustrates the first point, about universalization, with a discussion of promises and the following question: "ought I make a false promise in order to obtain some sort of short term gain?" For example, is it moral to borrow

---

[24] For example, Kant writes that "moral laws should hold for every rational being *as such*, the principles must be derived from the universal concept of a rational being in general. In this manner, all morals, which need anthropology for their application to men, must be completely developed first as pure philosophy … *independently of anthropology*" (*Foundations*, 28; emphasis added).

[25] Deborah Johnson, for example, misses it entirely in her explanation of killing in self-defense. See *Computer Ethics*, 30.

[26] "There is, therefore, only one categorical imperative. It is: Act only according to that maxim by which you can at the same time will that it should become a universal law" (*Foundations*, 38). Kant presents the second formulation as equivalent in content to the first.

[27] "The practical imperative, therefore, is the following: Act so that you treat humanity, whether in your own person or in that of another, always as an end and never as a means only" (*Foundations*, 46). This principle's derivation lies in the principle that moral actions are predicated on the autonomy of the human rational will; any act which did not proceed from the assumption of this autonomy would *ipso facto* not be moral. See *Foundations*, 44-45 and *Critique of Practical Reason*, 109-110.

$5 on the promise of repayment, when I have no intention of ever repaying you? Kant's answer is, of course, no, and the reason is that if I imagine that the principle – make a false promise in order to obtain something – were "a universal law," which is to say, true for all people at all times, then the institution of promising would cease to exist. This is because part of what makes a promise a promise is its credibility: if we all knew in advance that all promises were false, then we would never believe people who made them. In that case, says Kant, when I make a false promise, I am therefore also operating on a principle that would destroy promising itself. However, it is contradictory both to use the principle of promising and to destroy it at the same time. To making a false promise fails the test of universalizability.[28] I will discuss another common example, killing in self-defense, below. The important point is again to notice that one treats the "reason why" one does something as if it were always true for all people at all times – in other words, like a mathematical formula or a law of Newtonian physics (Kant wrote before Quantum mechanics).

The second formulation, that one should never treat others as merely a means, is easier to grasp. It is wrong to enslave someone, because that treats them as a tool for one's own gratification. This however does not respect their autonomy as a person. On the other hand, it is permissible to hire them to do work, because the exchange of money respects them as a person. This example is important, because the moral permissibility of such contracts is at the heart of our economic system.[29] Its advantages and disadvantages are of particular importance in the discussion of intellectual property rights, as will become apparent. On the other hand, it is equally important to modern thinking that people be respected *as* people, and not reduced to instruments for someone else's gratification. Another example of the means and ends distinction is provided by Gewirth's unfortunate citizen who is asked to torture his mother to appease a terrorist group. Citing this distinction in defending the person's refusal, Gewirth adds that using his mother's life as a means to appease the terrorists "subverts even the minimal worth or dignity both of its [the act of torturing's] agent and of its recipient and hence the basic presuppositions of morality itself."[30]

Thus for the Kantian formulation of deontology. Deontology has a tremendous intuitive appeal – it seems to square with a number of things most people instinctively think about morality: morality is about the actions of a person, it is important why that person did what they did, and it is important to respect others. The theory even captures the common childhood adage of "what if everybody did that?" Partly for reasons such as these, deontologists tend to take a dim view of utilitarianism. Indeed, from a deontological point of view, utilitarianism hardly seems worthy as a moral theory, since it seems to capture none of these features.[31] Deontology also enjoys a particularly strong following in computer ethics. For example, Eugene Spafford's famous "Are

[28] See Kant's discussion, *Foundations*, 38.

[29] And, it should be noted, the tendency to restrict the extent to which contracts can be freely undertaken even when they offend our sensibilities of what is right and moral has been an important change in the way American legal thought has treated contracts. See Chapter 3, "What is Property."

[30] "Are There any Absolute Rights," 226.

[31] Kant at one point says that "the direct opposite of the principle of morality is the principle of one's *own* happiness made the determining ground of the will" (*Critique of Practical Reason*, 32). See also: "it is a misfortune that the concept of happiness is so indefinite that, although each person wishes to attain it, he can never definitely and self-consistently state what it is that he really wishes and wills …. Omniscience would be needed for this …. The task of determining infallibly and universally what action will promote the happiness of a rational being is completely unsolvable …. Happiness is an ideal not of reason but of imagination" (*Foundations*, 34-45).

Computer Hacker Break-ins Ethical?" overtly argues from a deontological perspective. One may speculate as to why this is the case. One possible reason is the focus on formulas and algorithms: the theory is kept radically separate from the practice. If one formulates the principle correctly, then one has an algorithm for thinking about ethical issues. This can then be applied to the "data" of a given situation. Hence, insofar as computer ethics is a particular concern of those who work with computers – programmers and engineers, who are well-trained to formulate and apply algorithms – deontology's intuitive appeal is even stronger.[32] Although utilitarianism is also calculative, it tends to focus less on the formulation of principles.

The prevalence of deontology in the background of thinking about computer ethics may also help to explain the appeal of analogies. According to many versions of deontology, one always looks at theory over practice, which is to say not just that consequences are irrelevant, but also that the fact that people do or do not behave in a certain way is irrelevant to the consideration of whether they should. On the other hand, as we have seen, according to most of the popular definitions, the technological component is "essential" to computer ethics, which is to say that one cannot formulate a problem in computer ethics without attention to the very practical details of the hardware, software, and social environment. These two propositions are at tension with one another, because the second raises the possibility that problems in computer ethics are not amenable to the sort of formulaic abstraction that deontology favors.[33] One way to bridge the gap is by analogy: if one is able to say that problems in computer ethics are "new species of old problems," then one can use the "old" formulas. Analogies show how the new and old problems are related: computer hacking, for example, is "like" stealing. One is then able to use deontological prohibitions against stealing to condemn hacking. To use an analogy of a different sort, the simultaneous attraction and repulsion between deontology and computer ethics has a parallel in debates about program verification. According to one school, it is possible (or at least, very useful) to formulate rigorous, logically coherent, algorithmic representations of computer programs. That way, one *knows* that the program can or cannot fail. According to another school, the activity is a waste of time because real programs only operate on real computers. After they are translated into a high-level language, compiled, run on an operating system, and subjected to the vagaries of local power supplies and hardware specifications, real programs no longer can be adequately described by the algorithms.[34] The point here is not to take sides in what tends to be a very acrimonious debate; rather, the point is to notice how deontology can be thought as a way of approaching computer ethics.

Just as deontologists have been busy offering objections to utilitarianism, so have utilitarians offered numerous general objections to deontology. Some of the more common ones are: (a) an example based on killing in self-defense; (b) nobody actually behaves that way; (c) deontology is just lot of song and dance about intuitions; and (d) deontology collapses into utility. I will look briefly at each of these in turn.

After running through some examples of universalizing, it is common to arrive at the following objection to deontology. If I ask the question, "should I kill someone," the answer seems to be "no," because we could not rationally want a world where everybody killed everybody else: there would no longer be any people to do the killing. On the other hand, this seems to prohibit killing in self-defense. Surely this must be permissible, particularly in a moral theory that claims to be close to our intuitions? This objection

[32] This suggestion is made in Luciano Floridi, "Information Ethics."
[33] One can of course argue (and many do) that no ethical problems are amenable to such formulation.

[34] See William G. Lycan, "Response to my Critics," in *Digital Phoenix*, for one philosopher's account of his encounter with the topic.

actually is based on a misunderstanding of deontology. Recall that the point about universalization is that one universalize the *reason why* something is to be done, *not* the act itself. The objection here precisely attempts to universalize the act – killing someone – without asking why it is done. Hence, a correct formulation of the question is not "should I kill someone," but "should I kill someone because I saw them standing there?" *This* principle – "kill someone you see standing there" is clearly not universalizable. On the other hand, the principle "it is permissible to kill someone in order to save one's own life" clearly could be universalized, since the only people who would die would be those intending to murder in the first place.

The second objection, that nobody could act like deontology demands, has a standard answer to which Kant devotes considerable attention. The gist of it is that a theory about what people *should* do is useless if it confines itself to what they *actually* do. After all, the whole point of teaching people ethics is presumably to help them make "better" moral decisions. Kant answers a stronger version of the same objection – that no one in principle *could* be as moral as deontology demands – with the same answer: given that, on his argument, deontology is the only rational form of morality, and it is better to have morality than not, we should still hold ourselves to such high standards, even if we know we can never always reach them. We will still be better off as a species if we all try, however imperfectly.[35] One should recall, however, that one of the objections made to utilitarianism is that *utilitarians* demand more than human nature can provide. This may or may not be a fair objection, but it presumably is fair either to both camps or to neither.

The third objection, that deontology is glorified intuitionism, is based on the suspicion generated by the tendency of deontologists to announce that their results correspond to our moral intuitions. Surely something is suspicious about a theory that always justifies our intuitions? This is an example of what I meant when I suggested that utilitarians often call deontologists irrational. Furthermore, the difficulty in formulating one's principles correctly seems to be a natural point where intuitions might get in the way. For example, if I thought that women were not fully human and/or not fully rational (as many men thought (think?)), then I could justify their enslavement on deontological grounds: after all, deontology only proscribes actions against rational humans. One can think of similar examples about the disabled. If this is the case, however, deontology's claim to self-sufficient universality seems to be undermined, because at the very least, one needs to supplement it with a definition of "human." If that is the case, however, one is led to suspect that it will tend to be available to justify whatever intuitions the deontologist has, rather than to subject them to rational critique. Having quoted Nietzsche against the utilitarians, in the interest of fairness I will quote his mocking of Kant's discovery of a "moral faculty:" "is that - an answer? An explanation? Or is not rather merely a repetition of the question?"[36]

Finally, one can argue that insofar as deontology does provide a meaningful theory, that theory depends on utilitarianism. In responding to Mackie (quoted above, listing objections to utilitarian calculation), R. M. Hare suggests that, "it is indeed rather mysterious that critics of utilitarianism, some of whom lay great weight on the 'right to equal concern and respect' which all people have, should object when utilitarians show this equal concern by giving equal weight to the equal interests of everybody, a precept

[35] *E.g.*:"Nothing can secure us against the complete abandonment of our ideas of duty and preserve in us a well-founded respect for its law except the conviction that, even if there were never actions springing from such pure sources, our concern is not whether this or that was done, but that reason of itself and independently of all appearances commanded what ought to be done. Our concern is with actions of which perhaps the world has never had an example" (*Foundations*, 23-24).

[36] *Beyond Good and Evil* §12.

which leads straight … to utilitarianism itself."[37] In other words, if the premise of deontology is to respect each person equally, then this premise is shared by utilitarianism. Implicit in Hare's argument is the critique of deontology as irrational: the only way to rationally honor the insight that people are to be respected equally is through a utilitarian calculus.

In sum, neither deontology nor utility is a perfect ethical theory, in the sense that neither satisfies everyone who thinks about ethics, or even most people who think about ethics. However, both are important and influential, and either one or both operate in the background of much, if not most, thinking about computer ethics.

Rights

The idea of having a "right" is a familiar part of the U.S. political landscape. Indeed, the Declaration of Independence cites "inalienable" rights to life, liberty and the pursuit of happiness, and the "Bill of Rights" – the first ten amendments to the Constitution – enumerate a variety of others, although none of them are as explicitly tagged as "inalienable." That said, in most people's minds, a right is something which attaches to a person, and which cannot be taken away: if I have a right to life, then no one else is allowed to take away my right. If I have a right to free speech, then that means that I can say and publish whatever I wish. I cite the example of free speech because it shows the limitations to this common understanding of a right. One's speech *can* be limited by the government under certain circumstances. As we shall see, the government's efforts to limit pornographic expression on the Internet form an important focus for discussion of ethical issues in computing; understanding the ways in which rights – even "fundamental" ones can or should (or should not) be limited – is an important part of ethical and political thinking which will be recurrent in this text.

For now, I wish to establish a basic conceptual framework through which one can begin to think of the ethical implications of having "rights." As I suggested, according to a very common understanding, a right is something which attaches to someone simply because they are human. In this respect, we can immediately see the close connection between rights and deontology, since deontology is also concerned to treat people simply insofar as they are human. As it turns out, rights are often a criterion of deontology: we know that we have fulfilled our moral obligations to another when we have respected his or her rights. Conversely, when we understand what a person's rights are, we are much closer to understanding our moral obligations to him or her. From this, we can posit a basic definition of a right: having a right imposes a duty on someone else not to violate it. If I have a right to life, you have a duty not to kill me. This underscores an important point about rights: rights describe a relation between people. Many philosophers wish to extend the concept of rights to include (for example) animals and the environment. The rightness or wrongness of this approach is not of importance here. What is important is that the very fact that concepts such as "the rights of the environment" are viewed as an *extension* of rights indicates that the term usually applies to relations among people.

It is important to underscore that according to this understanding, rights function as criteria for measuring whether or not we have satisfied our obligations to others. The rights themselves cannot found the theory; with them, you need both some sort of theory of what it means to be human, and some sort of theory according to which this "human nature" is to be respected over other things or values. To say simply that there exists a "right to life" is question-begging: who has this right to life? Why should we respect it? Deontology frequently serves as the foundation which

[37] R. M. Hare, "Rights, Utility, and Universalization: Reply to J.L. Mackie," in *Rights and Utility*," 106-107.

answers these questions; rights then function as markers for knowing when we have met our deontological obligations.[38]

This basic understanding of rights leaves open a basic question: where do rights come from? How do I know that someone has a "right to life?" The traditional answer, one that dates to the Enlightenment, is that rights are "naturally" attached to humans, as part of what it means to "be human." Hence the wording of the Declaration of Independence: "we hold these truths to be *self evident*"(my emphasis). When something is said to be "self-evident," this means that it is taken as a basic principle, and the asking of questions stops here. John Locke, an English philosopher whose thought heavily influenced the drafters of the Declaration and Constitution, and whose thoughts about property formed the basis of the American system, expressed similar views. Whether you believe that this "natural" source of rights is God or nature, the point remains the same: the rights are part of being human. This position is also endorsed by many contemporary scholars. Among the more prominent of such advocates, the moral and legal philosopher Ronald Dworkin devotes considerable effort to grounding a theory of rights-based morality and politics on the minimal principle of equal respect for all people.[39]

This view has a strong intuitive appeal, and it certainly satisfies the deontological criterion that we respect people *as such.* The problem is that, even if you accept deontology as the framework for which rights are to be a criterion, the pronouncement that rights come "from nature" does not help very much in determining *which* rights a person has. Is the right to life natural? The right to free speech? The right to bear arms? The right to equal distribution of wealth? All of these positions have had their adherents. How do we sort them out? Deontology is not much help, since deontology only does the foundational work of saying that we should respect people, and that this respect is fundamental. Rights are supposed to be the criteria by which we know different ways that we can enact that respect. Now it seems that the rights themselves need criteria. Human beings, after all, can be lots of things. L. W. Sumner puts the point eloquently, so I quote him at length:

> The ambition of a natural-rights theory is to select that set of rights-principles that is most consonant with the natural facts. But *which* natural facts? To begin with, how do we decide *whose* nature is relevant? The answer within the natural rights tradition has usually been *human* nature, but how can we know that only our nature is relevant before we know which beings have rights? How then can

[38] It should be noted that rights can also be present in utilitarian theories, though deontologists tend to discredit their value there. For a programmatic summary of some of the difficulties in assimilating rights to a utilitarian theory, see Alan Gewirth, "Can Utilitarianism Justify any Moral Rights?" in *Human Rights*, 143-162. In brief, Gewirth's argument is that rights, defined as "necessary goods for action," *i.e.*, those things one must have (life, freedom) in order to be able to act at all, (a) are distributive, applying equally to all, rather than aggregative, in the manner of total utility maximization, and (b) more determinate, since a listing of preferences to be maximized by a utilitarian is "much more diffuse and eclectic" (151) than an enumeration of necessary goods for action. Based on this distinction, Gewirth argues that although rights could appear in a utilitarian theory, they could never found it or be essential to it. Hence, "even if the utilitarian calculus came out in such a way as to justify rules or institutions that require that each agent be given control over these goods [necessary goods for agency] for himself [that he or she be given them as rights], this is an accidental result" (154), since they are dervied from a principle of utility. For similar arguments, see Ronald Dworkin, *Taking Rights Seriously*.

[39] See his *Taking Rights Seriously* (Cambridge, Mass: Harvard UP, 1977).

> the scope of rights be determined by an appeal to nature? And if we do restrict our attention to human nature, which aspects of our nature are the relevant ones? We are beings capable of choice – do we therefore have a right to be free? We are also beings with subsistence needs – do we therefore have a right to the necessaries of life? If we have both rights, how does our nature determine which is to take precedence when they conflict? How in general can we distinguish between the relevant and the irrelevant aspects of our nature without presupposing a particular outcome for the argument? The problem here is not that no arguments are possible from natural facts to rights. The problem is that too many such arguments are possible and that there seems no way to arbitrate among them by further appeals to the facts.[40]

There is an additional problem relevant for the current context: "natural rights" do not do a very good job of describing how contemporary scholars think about issues such as intellectual property, privacy, speech, and so forth.

In response to problems such as this, one can argue that rights are fundamentally *political*, which is to say that they are founded in a political system. The right to life is only meaningful in a legal and political system which protects it. The general concept of "human rights" is only given meaning by the documents and discussions in which they emerge, for example, at the United Nations. In this sense, rights can be created by political process or by statutory law; fundamental rights are given in documents such as the Constitution. In this way, such a political understanding of rights avoids the difficulty in understanding where natural rights come from and therefore in how to assign them (they can be assigned politically – by democratic process, even). This political understanding also allows for more nuance than natural rights theories: given a conflict, one can reach a decision about *which* rights are more important. For example, perhaps the protection of people from dangerous working conditions is more important than their right to sign an employment contract according to which they agree to work in unsafe conditions. In law, this line of thought in fact developed partly in response to a Supreme Court opinion that the natural right to contract could not be taken away by labor laws.[41]

Natural rights advocates will immediately criticize this understanding of rights as inadequate: the whole point of having rights, the argument goes, is to *protect* people from the political system and from invasive social customs. Hence, founding rights within that system is fundamentally insecure. In response, one could argue that the phrase "natural rights" is itself meaningless, and actually could only ever refer to a political decision. That decision might be foundational – it could be in the constitution, use the word nature, and even say that the rights so enumerated are more important than anything else in the political system – but that fact should not obscure the fact that it is a political or social foundation.

I do not wish to delve further into this debate here, although a perusal of later chapters in this text will show that I am on the side against the natural rights theorists. Here I only to highlight a point which seems to underlie the debate about the origin of rights. In order seriously to defend natural rights, it seems, it is necessary that one be able to imagine people living outside of an organized society or system of laws. This is generally referred to as a "state of nature," and is regarded, for example, by Locke as an actual state of

---

[40] L. W. Sumner, "Rights Denaturalized," in *Rights and Utility*, 38.

[41] The case is *Lochner v. New York*, 198 U.S. 45 (1905). See the discussion in Chapter 3, "What is Property."

affairs describing the original state of humanity. On the other hand, one could also believe that it is impossible to imagine human beings living outside of society. If that is the case, then the concept of natural rights, at least in that form makes little sense.[42] The acceptance or rejection of a state of nature seems to lie at the root of much of the discussion of rights. This shown quite clearly in libertarian discussions which presuppose that less government is always better: the underlying assumption is that people can and should live in an a-political state, which means that the state of nature is both possible and desirable. This libertarian assumption is particularly prevalent in discussions of computers, as I have indicated in the first chapter.

A substantial percentage of the scholarship on computers and ethics can be divided into those who accept, implicitly or explicitly, something like the possibility and viability of the state of nature, and those who do not. At root is a fundamental disagreement on what it means to be human.

A discussion of rights would not be complete without mention of a criticism that can apply to any rights-based theory, no matter where one thinks the rights ultimately come from. This criticism, which is generally concerned with "rights trivialization," has more to say about the nature of debates about rights than the rights themselves. In political discussions in the U.S., rights are often played as a trump card: if I can establish that your policy or actions violate my rights, then that policy is presumptively invalid. There therefore arises a temptation to play this trump card too often, and to call things "rights" which perhaps should not be considered as such. The situation is rather like that of the boy who cried wolf. After enough false alarms, no one took him seriously any more. If every time I mean that something is "important to me," I attach the word "right" to it, then the word itself starts to lose some of its power. The consequence, in other words, of applying the term "right" to too many topics, is the dilution of the term itself such that it no longer carries the moral force we wish it to. The resulting "trivialization" of the concept of rights makes the term impotent in public discourse.[43]

Professional Ethics

The preceding sections have traced some of the thoughts that modern philosophers have applied to questions of ethics. These ethical theories have, in general, obscured what one might take to be a very important question: to what extent do the differing social roles that people bring to a situation effect their ethical relationship? For example, how would a king and a subject relate differently, from an ethical point of view, than two ordinary people? Or, more to the topic, to what extent does a lawyer or other professional have a special ethical relationship with his or her clients, colleagues, and members of the general public? Does it add something important to the description of an "ethical person" to know that he or she is an "ethical lawyer?"

In an important text on the subject, Alan Goldman puts the issue as follows:

[42] This is not to say that it is incoherent to base a theory on rights and to appeal to rights as a final justification. Dworkin makes such a move in articulating his "constructive model," according to which "Decisions taken in the name of justice must never outstrip an official's ability to account for these decisions in a theory of justice, even when such a theory mush compromise some of his intuitions. It demands that we act on principle rather than on faith" (*Taking Rights Seriously*, 162). Note that this position also attempts to deal with the objection that deontology collapses into intuitionism.

[43] See, *e.g.*, Mary Ann Glendon, *Rights Talk : The Impoverishment of Political Discourse* (New York: Free Press, 1991).

> The most fundamental question for professional ethics is whether those in professional roles require special norms and principles to guide their well-intentioned conduct. This is the most interesting issue from the point of view of moral theory, since its answer affects the structure of any complete moral system. It is also the most crucial for professionals themselves and for those who attempt to evaluate their conduct, since many decisions and evaluations in this area will differ according to whether special norms are required. For example, should lawyers ignore the interests of adversaries in pursuing their clients' objectives, in apparent violation of ordinary moral demands?[44]

One should note immediately that posing the issue in this way seems to invite the question of relativism. After all, the point behind modern ethical theories, insofar as they are constructed to avoid relativism, is that people should treat other people according to ethical codes which are independent of their social roles, that is, simply as human beings. Kantianism in particular seems committed to such a view, and even a utilitarian calculus would require considerable work to provide the sort of account Goldman describes. On the other hand, both philosophers since Aristotle and members of society in general tend to think that there is something worthy of thought in the relationship between, for example, a doctor and a patient. Not only that, most people would say that this doctor-patient relationship has characteristics which do not apply to other relationships between people. The legal system reflects just such distinctions, as for example by providing for confidentiality and the possibility of malpractice suits. These examples suggest an underlying thought, that doctors have a tremendous power over those in their care, and that with this power comes an increased responsibility for its fair and careful use.

Against this background, many have asked whether or not computer software programmers and engineers should be considered to be "professionals" in the same sense that doctors are, meaning that they have a social role which is sufficiently powerful that they should adhere to special norms of responsibility. On this question follows a separate, and distinct one: given an agreement that computer programmers should behave responsibly, to what extent should there be a binding code of ethics administered through some sort of professional organization (*e.g.*, the Association of Computing Machinery (ACM)), possibly even to the extent of providing a licensing procedure analogous to that for lawyers and doctors? At present, the ACM separates these two questions sharply: although it has adopted a code of ethics for its members who are software engineers, it strongly opposes any move toward licensing.[45] In May 2000, the ACM council:

> Concluded that the framework of a licensed professional engineer, originally developed for civil engineers, does not match the professional industrial practice of software engineering. Such licensing practices would give false assurances of competence even if the body of knowledge were mature; and would preclude many of the most

[44] Alan Goldman, *The Moral Foundations of Professional Ethics* (Totowa, NJ: Rowan and Littlefield, 1980), 1-2.

[45] See the code for software engineers at http://www.acm.org/serving/se/code.htm and the discussion below.

> qualified software engineers from becoming licensed.[46]

That said, the council added that "ACM believes the problem of reliable and dependable software, especially in critical applications, is the most important problem facing the IT profession."[47] How should one begin to sort out such issues conceptually?

Goldman suggests that a professional can be seen as having a "strongly differentiated" relationship with other members of society. Of course, everyone occupies social roles with one another, and these roles carry certain behavioral expectations. For example, waiters and customers at restaurants tend to follow rather standardized patterns of behavior with one another. Some roles, however, are more sharply defined than others. Those who have a strongly differentiated roles can almost be seen as defined by their roles, at least in this context. The paradigm case of such strong role differentiation is the family: almost everyone believes that family members have responsibilities and obligations to one another that they do not have to others in society. Indeed, when one thinks of a family member, one almost never thinks of them as an abstract "person," but almost always in their role as parent, child, etc.

Goldman suggests that the following considerations should be kept in mind when considering a case of strong role differentiation:

> The complete justification for strong role differentiation here requires that the institution in question serve a vital moral function in society. In addition, the elevation of the norm central to that institution, whether legal advocacy, health or profits, with its consequent limitation or augmentation of the authority and responsibility of the professional, must be necessary to the fulfillment of that function …. It must be shown that some central institutional value will fail to be realized without the limitation or augmentation of his authority or responsibility, and that the realization of this value is worth the moral price paid for strong role differentiation. That price is exacted from two sides. First, there are the interests or claims of others that are normally overriding but sacrificed to the demand of the professional norm, for example the interests of parties who oppose the lawyer's client. Second, there is the dulled moral perception of the professional himself, his insensitivity to interests that oppose the norm in question. This insensitivity may generalize into areas of conduct in which it can no longer be justified (7).

To carry the example through with families, almost everyone agrees that the family serves a vital moral function in society: it is not only the place where new members of society are produced, it is also (hopefully) one of the primary places where members of society develop their values. It is also (hopefully) a place where members of society can turn for support, moral and otherwise. The parenthetic insertions of "hopefully" serve to underscore the importance that we as a society attach to families: few political accusations have the rhetorical pull that accusations of causing the "breakdown of the family." Whatever they mean when they say the word "family," most people take it as an ideal of some sort.

---

[46] See the July 17, 2000 statement at http://www.acm.org/serving/se_policy/selep_main.html .
[47] *ibid*.

Within the context of families, it is also clear that families would completely fail to function without according family members special ethical roles with one another. For example, it is difficult to see how parenting could occur without giving parents more authority over their children than other members of society have over each other. That there are sharp debates about the boundaries and extent of this authority does not diminish the point that almost everyone, again, assumes that there should be some sort of parental authority. This feeling is sufficiently pervasive as to be deeply institutionalized: schools, for example, assume authority over children *in loco parentis* (in the place of parents), and when schools wish to take children on field trips, parents have to explicitly give the schools further parental power outside of school grounds in the form of a signed permission slip. The converse of this increased authority is an increased responsibility: it is not a crime to fail to feed a starving stranger, but it is a crime to fail to feed one's child. Child abuse and neglect are as painful to understand as they are precisely because they involve violation of a series of values fundamental to society.

Doctors also occupy an important social role. However, the boundaries of this role are less clear than those of families. In an obvious way, doctors have an explicit responsibility to use their knowledge, to the best of their abilities, to care for the well-being of their patients. Equally obviously, "health" is a fundamental social value. On the other hand, these points do little to clarify the need for and scope of a *professional* role for doctors. As the ACM points out, professional licensing assumes as one of its conditions the development of a body of knowledge which any licensed professional should have at his or her disposal (indeed, the mastery of an esoteric body of knowledge is generally taken to be one of the marks which differentiates a "professional" from other members of society). Even in the case of medicine, this poses questions: to what extent should doctors be required to "keep up" with research developments in their field? To put the negative version of the same question: when is a given treatment or procedure sufficiently well-established that *not* knowing about is a mark of professional irresponsibility? In a somewhat different vein, although children have a general obligation to obey their parents, what obligation to patients have to follow regimens of care proscribed by their doctors? These questions all become categorically more difficult when questions concerning the U.S. health care system – insurance companies, pharmaceutical companies, etc. – are brought into the picture.[48]

As the decreasing role differentiation from family to doctors suggests, part of the difficulty in understanding whether computer professionals are professionals in the sense that requires a "professional ethics," requires making a judgment about the extent to which the social role of computer professionals is sufficiently differentiated from other social roles. To answer this question requires an understanding of what the "social role" of computer professionals is. Unfortunately, this question is almost impossible to answer in a straightforward way. In an illuminating commentary, Michael P. Hodges points out that the question of "professional ethics" really requires addressing two related questions. One has to do with the institutional constraints within which the profession operates, and the other with an understanding of what the profession is as a "common practice or activity." In the case of computer professionals, the problem is that, as Hodges puts it, "what is at the center of the day-to-day life of many of those engaged in computing is not a single identifiable discipline but an object or group of

[48] For a subtle and sensitive introduction to the difficulties of making ethical pronouncements in medical situations, see Richard M. Zaner, *Troubled Voices: Stories of Ethics and Illness* (Cleveland, Ohio: Pilgrim Press, 1993). "Medical ethics," and "biomedical ethics" are vast and expanding fields.

related objects called 'computer technologies.'"[49] Indeed, we have already seen an aspect of this difficulty: it is difficult even to define "computer ethics" as a topic more precisely than to say it is at the intersection of people and computing technology. As computing becomes more pervasive in society, it seems less, rather than more, likely that one could arrive at a satisfactory disciplinary definition of those who use computers for a living.

The ACM position statement on adopting professional licensing points to one possibility of overcoming this difficulty. Suppose that one were to limit computing professionals to those who actually "create" the systems that others then use. In this sense, computing professionals would be a class of people that includes software engineers and programmers. One would then look for a code of conduct to guide such professionals. Indeed, as noted above, the ACM has produced just such a code. This obscures a further difficulty. How does one define excellence in computer programming? The answer to this question depends on whom you ask. Since the question is an ethical one, it has to indicate more than technical virtuosity. The ACM code, for its part, strongly emphasizes social responsibility. However, even the meaning of this can be contested. After all, many hackers insist that they are carrying out a socially responsible role by pointing out the security flaws in the computing infrastructure. This might not be a *good* argument, but to answer it requires defining what one means by social responsibility.

In the context of professionals, it turns out that this almost always has something to do with commerce. Furthermore, it turns out that a large part of the assumed good of commerce lies in its stability. From this point of view, the distinction between the hacker who is performing the social service of collapsing a network and the "computer professional" is that the latter behaves in a way which benefits the commercial operations of the network. For examples, hackers can and are often employed as computer security consultants precisely because they have the knowledge and ability not just to bring down sites and discover security holes, but to repair those sites and patch the holes. The hacker-corporate relationship moves from being that of criminal-victim to professional-client. It is with regards to this sense of professional-client relationships that one can perhaps most usefully think in terms of the "professional ethics" of those who use computers for a living. This approach also has the advantage of reflecting the values rapidly being codified in our legal system, which (as will be discussed) makes a fairly sharp distinction between unauthorized and authorized activity.

This model of professional ethics, then, is in a broad sense contractual: one aspect of how we define "professionals" in contemporary society is that they tend to enter relationships with clients, and that these relationships are determined by contracts. Such contracts can be implicit or explicit, but they are usually there. A doctor, for example, has a implicit obligations of care of his or her patients. Engaging the services of an attorney requires the development of a contract which specifies in a precise way the services which the attorney will provide and the amount the attorney will be paid. Such payment, for example, can be expressed an hourly rate, or as a percentage of any damage award by a court. The ethical computer professional, then, is one who honors explicit and implicit contractual obligations which occur as a result of his or her operating as any other "professional" participant in commerce. Indeed, the eight principles of the ACM code seem to reflect such a view.

On this view, the point for clarification is the nature of a professional-client relationship, and in particular of the division of decision-making authority between professional and client. There are several models possible, of which three will be discussed here.

[49] Michael P. Hodges, "Does Professional Ethics Include Computer Professionals? Two Models for Understanding," in *Computers and Ethics in the Cyberage*, ed. D. Micah Hester and Paul J. Ford (Upper Saddle River, NJ: Prentice Hall, 2001), 202.

They are the "paternal," "fiduciary," and "agent" and represent a sliding scale of decreasing professional and increasing client decision-making power.[50] These roles are not unique to computing, but can perhaps shed some light on it. Let me begin with an analogy to education. It is currently fashionable to speak of students as "customers" of a university. If this claim is to have any meaning at all, then it seems to suggest the assumption of a professional-client relationship between faculty and students. The faculty, who have all mastered an esoteric body of knowledge and who occupy a position of power relative to the students would be "professionals" in the sense relevant here. Students, who come to the university for the purchasing of educational services, would be clients.[51]

On a "paternal" understanding of this relationship, the university makes all the decisions, from the content of specific courses to course requirements. This is done because it is assumed that the students do not (yet) possess the relevant information and skills to decide for themselves how they are to be educated. The obvious risk of this position is that it might not meet the needs of students or might subject them to tyrannical professors pursuing their own agendas. On the other end of this spectrum, the faculty are understood as agents for students, and students make all of their own educational decisions, and have a right to expect such tangibles as good grades as a consequence of their expenditure of money. The difficulty with this view is that it is incoherent: if I begin by saying that I wish to acquire "education," then that assumes that I have a certain level of ignorance. Even if I knew what I wanted to know, there is no reason to think I would already know how, or how to measure when I had achieved "education." The analogy with law suggests another corollary of this position, usually unintended by those who advance it: the construction of a professional-client relationship as one of agency implies that the professional bears correspondingly less responsibility for a client who does not succeed. I can perhaps insist that my lawyer pursue a case that he or she thinks is a guaranteed loser, but I will have to pay in advance and will generally have little recourse when I lose anyway. In the middle is a fiduciary relationship, where decision-making authority is shared. One thinks in this context of distributional requirements: it is a requirement, for example, *that* students take a writing course, but it is up to their discretion *which* course they take.

A few points to take from this example. First, there is a substantial level of trust implied, and the level of trust increases as the professional has increased decision-making power. Parallel with the increase in trust is the obligation of the professional not to misuse or abuse that trust. In the context of computing and the prevalence of "guru" professionals, the trust placed in those who understand how to run computers is often very high. This is an almost necessary consequence of the combination of the importance of relying on the computer technology with the ignorance of most people in its operation. It would seem to follow from this that computer professionals have a high degree of professional responsibility to their clients. By extension, they would have an equally high degree of responsibility to society. For example, if a programmer knows that his or her company is about to release code which is dangerous – say, for example, it will be used in air traffic control, and contains errors – to what extent does he or she have a responsibility to resist that program's release, or, if that is not possible, "blow the whistle" and alert the public? Suppose that the programmer has a deep personal conviction against the usage of nuclear weapons, and he or she has been assigned to work on a nuclear weapons verification and testing system? These issues seem both to resist theoretical statement and to be important to the daily practices of computer professionals.

---

[50] See the discussion in Deborah G. Johnson, *Computer Ethics*, 45-48.

[51] I do not endorse this model. I wish to point out that it does not necessitate the conclusions that are usually drawn from it, and to use it as a topical introduction to questions of professional ethics.

CHAPTER III: INTELLECTUAL PROPERTY

Intellectual Property is among the most important and complicated issues in computer ethics. It is also one of the most volatile, in terms both of the speed with which the law changes and the intensity with which those changes are debated. In few areas have the capabilities of computers done more to threaten an established way of thinking. The questions involved are fundamental: if one is writing a program, to what extent can one "borrow" ideas from other programs? Is it unethical to make a copy of music one likes from a friend? How about from a stranger on the Internet? Does anyone have the right to own human genetic code? What would it mean to say that someone owns it to begin with? Does one have a right to one's name in cyberspace? These and other questions are within the general domain of intellectual property law. Many of them will turn out to have answers that seem not to immediately imply any fundamental ethical principles. The ethical principles will be at the root of them, but most of the concrete details seem to be worked out at the level of law. For that reason, I wish to begin this chapter with a bit of discussion of law in general. I will then follow with a discussion of property. After that, I will look at the main areas of intellectual property law as they apply to computers: patent, trademark, and copyright.[1]

What is Law?

Previous chapters have largely dealt with questions of computers and ethics at an individual level, from one person to another. However, as the discussion of professional ethics should indicate, it is at the level of society that many of these questions become important, both to be asked and to be answered. It becomes necessary not just to think of a code of conduct for one person, but for an entire society. Such a code of conduct can be thought of as a body of law. The relationship between "law" and "society" or "social values" is enormously complicated, and contested as a field of research.[2] Suffice it to say that many of society's values end up encoded into its legal system, and that many other values are not encoded into the legal system, and end up in efforts at critique and reform. One should also note that there are many possible ways of organizing a legal system or codifying a society's values, and that many sources other than laws can influence people's behavior. For example, the threat of strong parental disapproval has ended many a relationship, even when such relationship would be permitted by law. The discussion which follows is both brief and schematic, and is limited in that respect. However, it should suffice for the purpose which it serves here, which is as a backdrop for the following discussions of property law.

If you assume that society is composed of roughly equal, basically free (autonomous) individuals, then you have made the assumption which underlies the American legal system. This, more or less, is the founding assumption of "liberalism," although it is subject to many refinements and more precise formulations, many of which conflict with one another. One should note that this assumption is not necessary: if you are a Christian religious thinker,

[1] Because of space limitation and because the issues seem to be less unique to developments in information technology, I will not discuss questions of trade secrets in this chapter. For similar reasons, I will also omit discussion of ownership of "works for hire."

[2] See, for example, the debate surrounding the question of whether or not Supreme Court decisions spur social movements. The current round of this debate was started by Gerald N. Rosenberg, *The Hollow Hope* (Chicago: U. Chicago Press, 1991), which claims that empirically, they do not. For critiques of Rosenberg, see Neal Devins, "Review Essay: Judicial Matters: The Hollow Hope: Can Courts Bring About Social Change?" *California Law Review* 80 (July 1992), 1027-1069; and Peter H. Schuck, "Book Review: Public Law Litigation and Social Reform," *Yale Law Journal* 102 (May 1993), 1763-1786.

you probably believe that people's relationships with each other are *not* between autonomous, free individuals: rather, they are (or should be) determined by people's relationship with God and revealed law.[3] The American legal system's rejection of this foundation is shown in the First Amendment, and the Supreme Court draws the boundary sharply. For example, in a case decided in June, 2000, the Court ruled that it was not permissible for a public school to allow student led, public prayer. Since the school was a public, state supported one, and since students who did not wish to participate in the public prayer would be put in a very awkward position if they chose to attend the school-sponsored events at which such prayers were held, the Court ruled that the prayers, though student-led, amounted to governmental endorsement of their religious content.[4]

This case is useful in that it illustrates a couple of points. First, questions of law are often extremely complex, and turn on the interpretation of very fine details in the application of principles that may themselves sound easy. Hence, does it best uphold the principles of "freedom of religion" to endorse the freedom of some students to pray, or to endorse the freedom of other students not to be subjected to public prayers? Although it sounds easy to "just lock up criminals" or to say that "the prayer is voluntary," such easy solutions seldom provide useful material for resolving real problems. Indeed, when questions of fundamental rights are at stake, the court system generally rejects such broad solutions *because* they are overly broad, and apt to infringe on people's rights more than absolutely necessary.[5] Second, the controversy surrounding school prayer illustrates the extent to which the legal system reflects values which are contested in society itself. Furthermore, as social values change, so can their codification in the legal system. Again, the discussion here is of the U.S. legal system and society. Other societies, establish very different legal systems, and have very different values. For example, although questions of the "freedom of religion" are currently being debated in Iran, the terrain of the debate is entirely different, since the state is officially Islamic, and was founded on a rejection of Western liberalism.

The assumptions of liberalism can also be contested from other points of view. One important critique, made by many (feminists in particular) is that, since people only ever *actually* exist

[3] The *locus classicus* of this position in Christian Western Europe is St. Augustine, *City of God*. Augustine divides all people into those who are redeemed from original sin by following God's will and those who are damned because they don't: "For all the difference of the many and very great nations throughout the world in religion and morals, language, weapons, and dress, there existno more than the two kinds of society, which, according to our Scriptures, we have rightly called the two cities. One city is that of men who live according to the flesh. The other is of men who live according to the spirit. Each of them chooses its own kind of peace and, when they attain what they desire, each lives in the peace of its own choosing" (*City of God* XIV.1) It should be pointed out that Augustine's argument is that only those who live according to the spirit achieve true or everlasting peace – the "peace" of the kingdom of flesh is said to be wholly illusory.

[4] *Santa Fe Independent School District v. Doe*, No. 99-62 (June 19, 2000). Available online at: http://www.usscplus.com/current/cases/PDF/9900081.pdf.

[5] This doctrine is called "strict scrutiny," and says that if a law infringes on a fundamental right, it must (a) serve a compelling governmental need, and (b) be narrowly tailored to address that need, and (c) represent the "least intrusive means" available to achieve that need. Hence, as we shall see in the chapter on crime, the Court struck down the Communications Decency Act's prohibition on "indecent" speech online, because the term "indecent" was so vague as to encompass, and thus possibly prohibit, much more than the obscenity (pornography) that the law was theoretically designed to stop. Laws which do not involve fundamental rights are tested by the Courts according to less rigorous standards; the minimal is "rational basis," according to which the law has to address a legitimate governmental purpose, and to be rationally related to the achievement of that purpose.

in a society, then those who are disadvantaged by society should be protected by the law, and that the law's tendency to reinforce dominating and unfair social practices should be "unmasked" and critiqued.[6] At this point, liberalism turns out to be *unjust*, precisely because it refuses to recognize differences between people.[7] Again, the questions can become quite complex. For example, given that racism and sexism have had (continue to have?) a profound effect upon the abilities of "minorities" to achieve socially and economically, should there be some sort of compensation or redress built into the legal system? Liberalism can answer the question either way. On the one hand, one can argue that questions of social status are irrelevant before the law, the job of which it is to treat all people equally. On the other hand, one can argue that the function of law is to obtain "justice," and that part of justice is to see to it that each person is provided his or her due. Since that due is equal opportunity, it may be necessary to "level the field" through legal means. Those who critique liberalism can point to the failure of law to redress the injustice of racism and sexism as exemplary of the failure of liberalism. Even if one decides that some sort of legal redress is necessary, one can ask what form it should take. Should one adopt a program of "affirmative action?" If so, what sort? Or, should one address social spending to improve the standard of living of minority groups?[8] Finally, who gets to be included in this categorization? Homosexual people have been subject to a pattern of "invidious discrimination" but are not protected as are women and racial minorities.[9]

Liberalism is thus somewhat of a middle position, and American law tries to proceed from that foundation while admitting

---

[6] It should be stressed that "feminism" does not name a single ideology or set of beliefs; it is an important debate within feminist legal scholarship and feminist scholarship in general what the appropriate goals of a "feminism" might be. One of the most famous and controversial feminist legal critics is Catherine MacKinnon, who is well known for her work in favor of abortion rights, restrictions on pornography, and strict interpretation of standards for workplace harassment. For representative works, see her "Reflections on Sex Equality Under Law," *Yale Law Journal* 100 (1991), 1281-1328 and her *Feminism Unmodified: Discourses on Life and Law* (Cambridge, Mass: Harvard UP, 1987). MacKinnon is sharply critiqued by Judith Butler (who also rejects liberalism as I have just described it) in *Excitable Speech* (London: Routledge, 1997).

[7] This point is made with regards to gender in Seyla Benhabib, "The Generalized and the Concrete Other: The Kohlberg-Gilligan Controversy and Feminist Theory," *Praxis International* 5 (1986), 402-424. As a more general point about the need for law to attend to the "intersectional" nature of categories (race, gender, etc.) in which people live, see Kimberle Crenshaw, "Gender, Race, and the Politics of Supreme Court Appointments," *Southern California Law Review* 65 (March, 1992), 1467-1476.

[8] For an interesting comparison of American affirmative action programs with the parallel programs in Japan to improve the status of the Burakumin (descendants of an imperial grave-digger class), see Frank K. Upham, "Unplaced Persons and Movements for Place," in *Postwar Japan as History*, ed. Andrew Gordon (Berkeley: University of California Press, 1993), 325-346. Upham suggests that "as a result [of affirmative action], individual African Americans and members of other minorities have been able to gain positions of economic, social, and political power in society while the general condition of minorities has improved little if at all after the 1960s." In Japan, which did not have affirmative action but did have substantial social spending for schools and other infrastructure in Burakumin neighborhoods, "the result was the mirror image of the situation of African Americans. The ghettos where most Burakumin live were dramatically improved …. Viewed from the perspective of the individual, however, the situation was less promising. Despite the constitutional prohibition against state discrimination, there was no law banning private Buraku discrimination" (327).

[9] For a sustained critique of the implicit "heterosexism" in the legal system, see Sylvia A. Law, "Homosexuality and the Social Meaning of Gender," *Wisconsin Law Review* (1988), 187-235.

some of the insights of other positions. Thus, affirmative action, though violently contested in many quarters, has been an important component of employment law since the mid-1970's. Civil Rights Law has been expanded to protect women from sexual harassment in the workplace, though the boundaries of what constitute "harassment" are the subject of heated debate. One place where the tensions at the heart of liberalism come immediately to the fore is intellectual property law. The tension can be put as follows: copyright and other intellectual property law are designed to protect the original, creative works of authors. But those authors do not create in a vacuum; as any student of literature knows, and creative work involves borrowings from many other works. The law has both to respect the notion that authors are autonomous creating subjects, *and* to respect the notion that they both draw from and contribute to the "public domain" of information and ideas freely available to everyone. It is no wonder, perhaps, that many courts refer to this as a "delicate balance."[10]

Property and Contracts

Any society has to have a way of legally deciding what is mine and yours (*meum* and *tuum*, according to Roman juridical practice), and to have a way to enforce that distinction legally. Two important ways of deciding this follow from liberalist assumptions, property and contract. Both are fundamental to the operation of American society, and both entail similar assumptions. Their difference lies in their scope.

If "I" am relating to a "you" who is *any given* member of the public, or the public *at large*, one usually speaks of a *property right* which I have. The law then intervenes to make sure that "I" am protected from the encroachments of "others," and that a balance of my interests vs. those of others is maintained. The most famous classic example of this is provided by Locke in his *Second Treatise*: goods are held in common, until someone invests labor in them. Thus, one understands property as a relationship between a person and an object. That which I have worked on is mine, though this is specified in such a way as *to benefit society in general* (this last clause is important because many people try to forget it). I quote Locke at length:

> I think, it is very easy to conceive how labor could at first begin a title of property in the common things of nature, and how the spending it upon our uses bounded it. So that there could be no reason of quarreling about title, nor any doubt about the largeness of possession it gave. Right and convenience went together; for as a man had a right to all he could employ his labor upon, so he had no temptation to labor for more than he could make use of. This left no room for controversy about the title, nor for encroachment on the right of others; what portion a man carved to himself was easily seen, and it was useless, as well as dishonest, to carve himself too much or take more than he needed.[11]

Locke's formulation, though problematic from a contemporary perspective (see below) does contain two complications which are important. First, Locke makes an effort at specifying property in such a way that private gain and public good are balanced. This is of particular importance in intellectual property law; as we shall see,

[10] This tension is examined critically in James Boyle, *Shamans, Software and Spleens* (Cambridge, Mass: Harvard UP, 1996).

[11] John Locke, Second *Treatise on Government*, in *The Works of John Locke* (London, 1824), IV, §51.

the Constitution specifies exactly this balance. Second, Locke's text implies a prohibition against monopoly, which is to say that Locke implies that it is wrong for one agent to take over an entire market. The relevance to issues in computers is clear, as the Department of Justice's Case against Microsoft poses just such a question.

More specifically, Locke assumes that the supply of things in the public is unlimited. If, however, as seems really to be the case, there is a finite supply of goods, then it is bad for one person to own all of them. This hurts society in general, because that person has a *monopoly* and can charge unfair prices, etc. I mention this now because anti-trust (anti-monopoly) principles are at work in a lot of the thinking about intellectual property, even when they are less obviously at play than in the Microsoft case. Indeed, intellectual property is conceived as a "limited monopoly" right granted to the author. It thus attempts to balance the advantages of the incentives to work that monopoly creates, with the disadvantages that monopoly entails.

Computer property questions usually concern "intangibles," and most importantly, "intellectual property," which is protected by a series of "intellectual property rights" (IPR's). In one sense, intellectual property adheres to the fundamental Lockean idea of "work:" the idea is to protect an investment while promoting the public good. In another, it departs radically from this Lockean understanding because the relationship is not understood as between a person and an object, but rather as a relationship between people and *about* a resource. In this sense, property names a "bundle of rights" describing how people can be included in and excluded from use of that resource.[12]

If, rather than relating to anyone in general, "I" am relating to a specific "you" with whom I have a legally specified relationship, then some sort of *contract* governs that relationship.[13] The basic point is that it is necessary to have a way to ensure that people keep their promises, and that they can be penalized if they do not. The need can be justified on economic terms: if it takes me a week to produce a widget which you need for a product that takes you a month to produce, you will need the widgets from me before you have the revenue to pay me for them. You will also need to know that I will make the widgets available to you on a regular basis, so that you in turn can promise to supply your product to others. The different production times, in other words, require an enforceable system of payments and promises for supplies. As many commentators have noted, one of the difficulties for economic recovery in the former Soviet Union has been the lack of a developed system of contract law, and a lack of ability or willingness on the part of the government to enforce the system that exists. Of course, one can also have non-economic contracts: a marriage license, for example, represents a contract between two people. This is why it is necessary to bring legal action to obtain a divorce: unlike breaking up with a boyfriend or girlfriend, ending a marriage requires proving why one or both partners is not fulfilling the contractual obligations implied in the marriage contract.

In principle, anyone can contract with anyone else. This, at least, was the governing principle behind most enlightenment-based political philosophy. This principle encountered difficulties in the industrial revolution, however. Legally, taking up a job generally

[12] This understanding is explored and criticized at length in J. E. Penner, "The 'Bundle of Rights' Picture of Property," *UCLA Law Review* 43 (February 1996), 711-820.

[13] Some thinkers (Locke, Hobbes, and Rousseau are the classic examples of this) take the contract to be a model for society in general ("social contract theory"). According to such a theory, society can be viewed as created by an "original contract" of its members to transfer some of the rights they would have outside of society to a governing agency, in order to secure their common protection. In other words, "contract" can be a useful analogy in legal philosophy, even when a contract does not technically apply.

involves an employment contract. Economically, it was (is) desirable, from the employer's point of view, to pay people as little as possible, particularly for unskilled work. This led to the widespread adoption of unsafe working conditions, very lengthy (twelve and more hour) working days, child labor, and so forth. These practices continue to be desirable to employers, as evidenced by the need for international campaigns against clothing manufacturers who produce their products in overseas sweatshops. One response to these problems on the part of social reformers was to pass legislation which limited the use of child labor, limited the maximum number of hours in a working day and week, provided a minimum wage, and so forth. Since apparently "self-regulation" was not sufficient to ensure a human existence for workers, reformers advocated state intervention. However, such state intervention necessarily limited the capacity of employers and laborers to contract. An early result was the now infamous Supreme Court decision in *Lochner v. New York*,[14] which invalidated a statute restricting bakers to a sixty hour work week (10 hour work day). Complaining that "this interference on the part of the legislatures of the several States with the ordinary trades and occupations of the people seems to be on the increase" (63), the Court concluded of the New York statute that:

> It seems to us that the real object and purpose were simply to regulate the hours of labor between the master and his employees (all being men, *sui juris*), in a private business, not dangerous in any degree to morals or in any real and substantial degree, to the health of the employees. Under such circumstances the freedom of master and employee to contract with each other in relation to their employment, and in defining the same, cannot be prohibited or interfered with, without violating the Federal Constitution (64).

No doubt the Court was correct as to the purpose of the statute. From the point of view of classical liberalism, the decision makes perfect sense. After all, why should one interfere with the rights of people to contract? The problem, and the reason that Lochner became notorious, lies in the courts assumption that "master and employee" should be understood to have the same sort of relation as people *sui juris*, *i.e.*, people of equal right taken as such. The relation of employer and employee, however, as subsequent law has come to recognize, involves a substantial power differential. The employee does not necessarily "choose" to work more than sixty hours a week any more than a woman "chooses" to work in an office which harasses her. It may be the case that this is necessary for the employee to support a family, just as it might be the case that sexual harassment is pervasive, but it does not follow that either state of affairs is desirable. It also does not follow that the employee could have freely chosen to work a job without such problems. As anyone who has applied for jobs knows, jobs in the same profession tend to have approximately the same wages and working conditions.

Contracts, then, present a tension for thinking about ethics and political philosophy. On the one hand, as foundational constructs in our philosophical and legal system, contracts are the device whereby free people choose to enter into relations with one another, according to their individual preferences. On the other hand, the very prevalence of contracts in society and the necessary existence of inequalities between people, makes it equally possible to question the actual freedom of people to choose to enter or not to enter various contractual relations.

[14] *Lochner v. New York*, 198 U.S. 45 (1905). References here are from this case.

The question of freedom of contract is of particular currency for computer software. Increasingly, purchasing software requires agreement to a "license." Indeed, technically, one does not "purchase" such software at all, but instead licenses to use it. For example, to install most programs, one must first click "I agree" to a lengthy series of licensing terms. Software companies assert that these "shrink-wrap" or "mass-market" licenses are necessary to protect their products against, for example, illegal copying. Since copying is so easy, and since people will tend to use the products in a manner different from the software companies' intents in developing them, it is necessary to have new legal protections for the company's substantial investment in software development. Hence, for example, users might be required to agree to the software's only being run on one machine, and that the software could stop itself from being copied to another. Customers who object to these provisions are free not to use software which comes with them. On the other hand, many commentators, citing similarity of the "freedom of contract" arguments made by software companies to the mindset of the Court in *Lochner*, assert that these contracts are hardly freely made. Not only do all companies have an economic incentive to adopt the same licensing procedures (meaning there is nowhere to go for those who object to the provisions), but also consumers do not have the purchasing power to contest such agreements. Hence, the idea that agreement to mass-market licenses is "chosen" is illusory.[15]

At present, the future of these mass-market licenses is up in the air. The software industry has heavily lobbied for passage of Uniform Computer Information Transaction Act laws which would give the licenses legal validity. On the other hand, in the states where the licensing laws have passed, public criticism has forced either delay of the provisions or the addition of clauses providing greater consumer protection.[16] The mass-market licenses also illustrate explicitly the difference between property and contract law, since they are designed to supplant intellectual property law. Rather than purchasing a copy of a piece of intellectual property, the software consumer is contracting to use the product in specified ways.

The U.S. Legal System and Jurisdiction

A bit more about legal theory and the structure of the American legal system will help the following discussion. Again,

---

[15] I critique these licenses in my "On the Fetishization of Cyberspeech and Turn from 'Public' to 'Private' Law," *Philosophy and Social Criticism* (under consideration). I have drawn extensively from David Nimmer, Elliot Brown and Gary N. Frischling, "The Metamorphosis of Contract into Expand," *California Law Review* 87 (1999), 17-77. Nimmer is criticized by Joel Rothstein Wolfson in "Contract and Copyright are Not at War," *California Law Review* 87 (1999), 79-110. See also the criticisms in Charles R. McManis, "The Privatization (or 'Shrink-Wrapping') of American Copyright Law," *California Law Review* 87 (1999), 173-190; in Julie E. Cohen, "Copyright and the Jurisprudence of Self-Help," *Berkeley Technology Law Journal* 13 (Fall 1998), 1089-1143; and the critique of the ideology behind regimes such as UCITA in Julie E. Cohen, "Lochner in Cyberspace: The New Economic Orthodoxy of 'Rights Management,'" *University of Michigan Law Review* 97 (November, 1998), 462-563.

[16] At present, Virginia and Maryland are the only two states to have passed UCITA laws. Maryland diluted considerably some of the powers available to manufacturers, and Virginia delayed implementation for a year to study those powers. See "Md. software law expands protection for consumers," *USA Today* (April 27, 2000), 3D; and "Software law could be a hard sell," *USA Today* (March 29, 2000), 3D. For discussion of UCITA as part of Virginia's bid to become "Internet capital of the world," see Craig Timberg, "Gilmore Signs Bill On Software; State Is First to Enact Industry-Backed Law," *Washington Post* (March 15, 2000), B01. For a general discussion and criticism of the status quo provisions, see Joseph Menn, "Software Makers Aim to Dilute Consumer Rights," *Los Angeles Times* (Feb. 4, 2000), A1 (financial desk).

what follows is very schematic, and not to serve as a replacement for a more detailed discussion of government. However, it should serve to highlight some basic issues which are in the background of discussions of computers and law, and to highlight some of the difficulties of applying law to information technology.

Law can have several main sources. Among them are statutory, case (judicial), and common law. All three are relevant in the following. All are involved with interpretation and application of the Constitution. Statutory law, which happens when legislatures pass laws, should be sufficiently clear. Common law, which has to do with customs being so common and normal that they have the status of law, is not generally relevant in the context of computers, since the technology is so recent. The mechanisms of judicial law are worth review, however. Federal judicial law is made through court decisions. These create a *binding precedent* in whatever jurisdiction they are decided. Other courts can also cite them as evidence in support of their reasoning. Federal Court decisions begin in district court. These are appealed to the Circuit Courts, of which there are 12. Those decisions are appealed to the U.S. Supreme Court. A higher court's decision automatically overrules conflicting lower court decisions. On questions of constitutional law, a court's decision can also invalidate a state or federal law if the court finds that law to violate the constitution. So, for example, the Supreme Court's decision in *Roe v. Wade* invalidated all state laws which outlawed abortion, as well as all lower court precedents which upheld those laws as constitutional.[17] Subsequent cases about sexual privacy cite *Roe v. Wade*, including those that allow state restrictions on abortion rights (such as requiring minors to notify a parent).[18] One of the main problems in computer law at the moment is the paucity of clear Supreme Court decisions, as the circuit court decisions often conflict. For example, there is not currently a Supreme Court decision about the many difficulties which confront trademark law when applied to the Internet.

The U.S. is a federalist system, which divides power between the states and the federal government. The division of those powers is the subject of many academic and legal careers; a couple of points should be noted for the following.[19] First, IPR's (in this case, trademark, patent, and copyright) are generally protected as a matter of *federal* law. The §301 of the Copyright Act of 1976, for example, explicitly pre-empts (takes the place of) any state law which duplicates its provisions or speaks to exactly the same topics. Contracts, on the other hand, are generally regulated as a matter of *state* law. Similarly, although states have considerable jurisdiction within their own borders for such things as consumer protection laws, commerce which occurs between states is regulated by federal law. Given that the Internet crosses state lines so easily, and given that much of the computer industry is national in scope, one of the more difficult questions emerging in computer law has to do with when federal law preempts state laws. We have already seen one example of this, as some scholars have argued that state laws allowing mass-market licenses are so close in their scope and intent to federal copyright law that they should be pre-emted.[20]

From the point of view of making policy, each of the sources of law can be said to have disadvantages. Legislative policy (statutes, laws) is (a) notoriously slow to enact because if the

[17] *Roe v. Wade*, 410 U.S. 113 (1973).
[18] *Planned Parenthood v. Casey*, 505 U.S. 833 (1992).

[19] A common complaint is the expansion of federal power at the expense of the states. For the argument that one consequence of the development of the Net will be a further diminution of state autonomy and power, see Walter Russell Mead, ""With New Technology, Federal Control Always Grows – But Wait," *Los Angeles Times* (February 27, 2000), M1.
[20] See David Nimmer, Elliot Brown and Gary N. Frischling, "The Metamorphosis of Contract into Expand," and the criticism of them in Joel Rothstein Wolfson, "Contract and Copyright are not at War" for a debate on this topic.

question is at all complicated, it requires compromise between many groups with wildly divergent opinions; and (b) prone to inordinate influence by special interest groups. For example, when Congress passed the Communications Decency Act in 1996, much of their evidence was based on a law journal article dealing with Usenet chat groups, a form of communication which no longer describes the bulk of communications on the Net, much less the bulk of "indecent" communications on the net.[21] Legislation about computer crime is even more prone to lag "behind the times." Examples of special interest group influence can clearly be seen in the structure of emerging intellectual property law, which heavily favors the desires of the well funded and organized lobbying of the Motion Picture Association of America (MPAA) and Recording Industry Association of America (RIAA). Examples outside of the computer industry are also easy to find: for example: the National Rifle Association (NRA) seems to have Congress in its pocket, even though neither gun manufacturers nor a majority of Americans favor the NRA's interpretation of the 2nd Amendment. Vote buying by the tobacco, entertainment, and anti-Castro industries is also frequently noted. While this does not necessarily require cynicism about elected government in general, it does mean that the process of achieving legislative policy decisions is very complicated, and requires compromise with powerful lobbying groups.

Judicial policy suffers from several possible disadvantages: (a) critics of "judicial activism" assert that it is undemocratic because (federal) judges aren't elected;[22] (b) it requires a "case in controversy" – *i.e.*, a challenge to a law or a challenged situation, before a ruling can be reached. In the meantime, an existing law, no matter how bad, will influence people's behavior; and (c) it is slow, particularly in the appeals process, to the point that the facts relevant for understanding a case may change between an initial decision and its review by a higher court.[23] The court's opinion has to negotiate a difficult dilemma. If the opinion is too broad, it risks being overrun by changing technology in the sense that the broad opinion seems not to fit rapidly changing sets of facts. If the court avoids this problem by tailoring its decisions narrowly to the facts at hand, it risks undermining their precedential value. Courts have tended to take the second approach, of writing decisions narrowly tailored to the facts at hand, and one consequence has been that it has been hard to apply those decisions to subsequent cases.

---

[21] See the discussion of Pornography in chapter 5, "Computers and Crime."

[22] This debate is of long-duration and often acrimonious. Currently, Supreme Court justice Antonin Scalia is one of those who insist on "strict construction" of constitutional and statutory terms as a hedge against judicial policy-making. Another "originalist" is Reagan Supreme Court nominee Robert Bork. His position is outlined in Robert H. Bork, *The Tempting of America: The Political Seduction of the Law* (New York: Free Press, 1990). Among numerous critiques of Bork, see for example, Stephen Macedo, "Originalism and the Inescapability of Politics," *Northwestern University Law Review* 84 (1990), 1203-1214. For an "activist" understanding of statutory (as opposed to constitutional) interpretation, see William Eskridge, *Dynamic Statutory Interpretation* (Cambridge, Mass: Harvard UP, 1994).

[23] For example, the Microsoft antitrust case depends on the following findings of fact, which many think may change soon: (a) the lack of market share for Linux, (b) the dominance of Intel-based PC's as a platform for computing, (c) the viability of a distinction between an operating system and a browser. Internal Microsoft documentation suggests that the corporation is particularly afraid of open source software (OSS) in general and Linux in particular (lending credence, perhaps, to the charge that the DeCSS Copyright prosecution is a red herring for special interest groups in the software industry). If any of these facts change within the next couple of years, the basis for a heavy penalty against Microsoft, supported by the facts at present, would go away. These issues are discussed at length in Stuart Minor Benjamin, "Stepping into the Same River Twice: Rapidly Changing Facts and the Appellate Process," *Texas Law Review* 78:2 (December 1999), 269-373, especially at 300ff.

The executive branch (President, FBI, etc.) can also be a source of law, and many advocate the idea that the executive branch, through executive orders or administrative policies, should create *de facto* laws about computers. Certainly it does, whether in the form of FBI policies to fight crime to the Department of Justice's suit against Microsoft. While executive policymaking addresses questions of speed, it raises in particularly acute form questions of (a) separation of powers between the legislative and executive branches, (b) whether such *de facto* laws are really binding in the same way congressional laws are. Both of these issues can be seen in the highly politicized question of Internet domain names. Facing a shortage of available .com names, the Clinton administration established an international body called ICANN (Internet Corporation for Assigned Names and Numbers) to develop a series of guidelines for developing new systems for Internet addressing. Congressional critics have suggested that the administration exceeded its authority in setting up ICANN, doing something that Congress was constitutionally assigned (the regulation of commerce).[24] It is also worth noting that ICANN poses questions of sovereignty: members of ICANN will be elected internationally, a state of affairs which will likely lead to a quasi-governmental organization having substantial control over e-commerce. Also, with the new domain names developed by ICANN, the importance of the American controlled .com names would likely diminish. As the French newspaper *Le Monde* put it, this would be "a sharp change from a time when most of the organisms or associations of Internet regulation are populated by Americans."[25]

Questions of jurisdiction, which are related to questions of sovereignty, and which cover where a case is heard, and whose laws govern, are complicated, even given the outlines above. For example, can a California pornographer be liable for content provided online which violates the laws of the state or country to which it is sent, even if it is legal in California? One 6th Circuit Court case said upheld the conviction of such a California couple whose products violated Tennessee obscenity laws.[26] On the other hand, the court specifically avoided addressing the real jurisdiction question because the California couple operated a subscription only bulletin board service, and part of the subscription process involved both mailing something to the new subscriber and phoning him. Hence, the couple knew their material was going to Memphis, and argued that ignorance of the law is no excuse.[27] The real question, of course, concerns what happens when one does not know where the material is going (for example, it's posted on a WebPage), and the legal and ethical questions surrounding this have yet to be resolved.

One emerging legal standard for jurisdiction concerning websites in the U.S. and their users is based on how actively a person engages a website. The more interactive the website, the more likely the location of the user will have jurisdictional authority over the website. The more the website is passive, or users merely look at it, the less authority their local legal system will have and the more the system where the site is operated. This standard was articulated by a district court as follows. After cautioning that "the development of the law concerning the permissible scope of personal jurisdiction based on Internet use is in its infant stages" and that "cases are scant," the court adopts a sliding scale:

> The likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that

[24] See "New domains at last," CNN.com (June 27, 2000).
[25] "*Internet, un vote pour la régulation*," *Le Monde* (June 28, 2000).
[26] *U.S. v. Thomas*, 74 F.3d 701 (1996).
[27] *U.S. v. Thomas*, 711-712.

> an entity conducts over the Internet …. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction is proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.[28]

Two examples will serve to clarify. The first is the case cited by the *Zippo* court as exemplary of proper personal jurisdiction. In *CompuServe v. Patterson*, Patterson (who lived in Texas) entered into a contract with CompuServe (headquartered in Ohio) to market a shareware program which he wrote. When CompuServe marketed a similar program, Patterson asserted that the program's name violated "common law trademark," which is to say, that although Patterson had not specifically applied for trademark protection (see below) for the software, nonetheless, CompuServe's program was sufficiently similar as to confuse consumers who were looking for his. CompuServe then changed the name of their program; when Patterson continued to complain, CompuServe filed suit asking for a declaration by the court that CompuServe was not violating any trademarks owned by Patterson. Part of Patterson's response to this request was to claim that since CompuServe filed its suit in Ohio, and not only did he not live in Ohio but he had never even been there, Ohio had no jurisdiction over him. The District court in Ohio accepted Patterson's argument and rejected CompuServe's petition. On appeal, the 6th Circuit Court argued that this ruling was mistaken: Patterson had knowingly entered into a contract with an Ohio-based company to market his software, and that was sufficient grounds for CompuServe, as that Ohio-based company, to sue him in Ohio courts under Ohio law. As the Circuit Court said, "Patterson has knowingly made an effort – and, in fact, purposefully contracted – to market a product in other states, with Ohio-based CompuServe operating, in effect, as his distribution center. Thus, it is reasonable to subject Patterson to suit in Ohio, the state which is home to the computer network service he chose to employ."[29] The Circuit Court then sent the case back to the lower court for reconsideration, since it was now in their jurisdiction.

The second case, *Mink v. AAAA*, also about intellectual property law, cites *Zippo*. In this case, Mink, a Texas resident, had developed a computer program to assist his operation of a retail furniture business, and filed for copyright and patent protection. He shared his ideas at a trade show, and they eventually found their way to AAAA, based in Vermont. Mink argued, among other things, that AAAA had copied his programs, and that because their website was visible from Texas, it was proper for him to file suit against them in Texas. Here, the 5th Circuit Court affirmed a lower court ruling that the mere possibility of visiting a website in Texas was not enough to contact to establish jurisdiction in Texas. Citing

[28] *Zippo Manufacturing Co. v. Zippo Dot Com*, 952 F. Supp. 1119 (WD Pa), 1123-1124, citations omitted.

[29] *CompuServe v. Patterson*, 89 F.3d 1257 (1996), 1263.

the passage of *Zippo* quoted above, the Court reasoned that "essentially, AAAA maintains a website that posts information about its products and services. While the website provides users with a printable mail-in order form, AAAA's toll-free telephone number, a mailing address and an electronic mail … address, orders are not taken through AAAA's website." They added that therefore, "this does not classify the website as anything more than passive advertisement which is not grounds for the exercise of personal jurisdiction."[30]

Jurisdiction, in short, is a question which is difficult to settle in advance. Nonetheless, the courts seem to be moving to a standard for websites which is based on the degree to which actual business is conduced over the Internet. The more an Internet transaction looks like a real world transaction, the more likely the courts will grant jurisdiction to a plaintiff in his or her home jurisdiction. One should also note that these cares are of intellectual property law: one of the most contentious and difficult issues posed by the emergence of the digital economy.

Patents

Patents are perhaps the easiest of the intellectual property rights to understand conceptually. Ordinarily, one would say that monopoly is bad, because monopolies discourage innovation and competition, thereby hurting both individual consumers and society. As the sheer length of the rulings in the Microsoft antitrust case illustrate, the exact specification of monopoly is complicated. According to Justice Jackson, to constitute an illegitimate monopoly, a company would have to (a) have a monopoly share in a relevant market, and (b) seek to retain or augment that share through "anti-competitive means." The latter might include setting prices at artificially high (or low) levels, behaving aggressively to stop potentially competing products to enter the market and so forth, and is to be distinguished from market share gained through superiority of the product, business acumen, and the like.[31] In this respect, anti-monopoly (anti-trust) measures are designed to foster innovation and competition, which in turn will benefit consumers, who will have access to better and cheaper products.

Suppose, however, that a company spends its money developing a new cancer drug. This drug represents a significant investment on the part of the company, which hopes to recover its expenses through sales of the drug. However, the day the drug hits the market, competing companies take it to their laboratories, learn its chemical composition, and soon market competing products. These competing companies, because they did not spend any of the money researching the drug, are able to offer it much more cheaply. Hence, the company which spends the money researching the product gets no return for the research, and therefore has no incentive to conduct such research. In fact, the company has an incentive to wait for someone else to market the drug, since free-riding off another company's research would always be more profitable. If everyone thought this way, then consumers (cancer patients) would suffer, because the nature of competition in the market would discourage research into new treatments.

Patent law is designed to remedy such a situation by offering an inventor a "legitimate monopoly" on the use of his or her invention. The owner of a patent has exclusive rights, for a limited time, to market the product covered by the patent. One notices that this is an anti-competitive measure to maintain market share: anyone who copies and markets the product can be sued in court, which has nothing to do with product quality or business acumen. However, the idea is that such an anti-competitive measure, in this case, actually serves the public by giving inventors an incentive to pursue their research. If I know that I can be the only one who will profit from my research for a given period, then it

[30] *Mink v. AAAA Development*, 190 F.3d 333 (1999), 337.

[31] *U.S. v. Microsoft*, Conclusions of Law (April, 2000), 4.

becomes worth my time to conduct that research. The interests of the public, and of the market, are in turn protected by limiting the duration of patent protection (17 years in U.S. law). Hence, at least in theory, everyone benefits: I get to profit from my work, but the public gets the innovative product after a reasonable period.

In order to qualify for patent protection (it is a laborious process to apply for a patent) and to have my patent upheld in court, my invention must first of all be patentable, and then also (a) have utility, (b) have novelty (not be an example of a "prior art"), and (c) be nonobvious. Let us deal with the latter three criteria first. Something which has utility is useful in some way. In other words, since patents are designed to promote scientific and industrial progress, one cannot obtain patent protection for something which is itself useless. Second, the patented product must actually present an innovation. An inventor cannot attach his or her name to a process or product which has been in common use and thereby gain the right to all profits from it. This requirement is not as straightforward as it seems, and there is considerable controversy over whether, foe example, pharmaceutical companies should be able to patent drugs developed from tropical plants which have been used by indigenous healers for centuries. On the one hand, the extraction and replication of the chemicals in the form of a pill is clearly conducted by the pharmaceutical company. On the other hand, the art itself – healing with the chemicals, albeit in a different form – has been practiced by the indigenous people for hundreds of years.[32] Finally, the product or process must be non-obvious: I could not patent the process, for example, of making a shopping list, because even if no one had done so before, the idea is obvious.

A case illustration will clarify. *Amazon.com vs. Barnesandnoble.com*[33] concerned Amazon.com's patent on "one click shopping," in which returning customers could press a single button onscreen, and complete the entire ordering process at once. Basically, Amazon won a "preliminary injunction" against bn's "express lane" feature on the grounds that if probably violated of amazon's patent. Barnesandnoble.com was ordered to cease and desist use of the "express lane" feature pending the resolution of amazon's case against them.[34] The court found that a fuller analysis of the case would likely show that (a) amazon.com developed this new way of ordering online; (b) the single click addressed a huge problem in online commerce, the number of people who departed a web page without actually making it to the "checkout," leaving their "shopping carts" with products

[32] See the discussion below, as to what is or is not patentable. See also the strange cases discussed in James Boyle, *Shamans, Software and Spleens* (Cambridge, Mass and London: Harvard UP, 1996), 97-107, *et passim.*

[33] 73 F. Supp. 2d 1228 (WD Wa, 1999).

[34] An "injunction" is an order of the court. A "preliminary injunction" is one which is issued prior to the full trial of a case and can be granted under patent law when the moving party meets four conditions "(1) reasonable likelihood of success on the merits; (2) irreparable harm; (3) the balance of hardships tipping in its favor; and (4) the impact of the injunction on the public interest.' *Hybritech, Inc. v. Abbott Labs*, 849 F.2d 1446, 1451 (Fed Cir. 1988)" (cited in *Amazon*, 28-29). *Cf*. a recent Supreme Court discussion of a preliminary injunction: "The purpose of a preliminary injunction is merely to preserve the relative positions of the parties until a trial on the merits can be held. Given this limited purpose, and given the haste that is often necessary if those positions are to be preserved, a preliminary injunction is customarily granted on the basis of procedures that are less formal and evidence that is less complete than in a trial on the merits. A party thus is not required to prove his case in full at a preliminary-injunction hearing, and the findings of fact and conclusions of law made by a court granting a preliminary injunction are not binding at trial on the merits" (*University of Texas v. Camenisch*, 451 U.S. 390, 395 (citations omitted)).

contemplated but not actually purchased;[35] and (c) the single click was not obvious. [36] The first part could be established with reference to the fact that Amazon.com actually obtained a patent on the process. The second and third relied on the court's interpretation of expert testimony provided by both parties.

As the preceding case shows, one advantage of patent protection is its strength: simply because it had a patent on the 'one-click' shopping, Amazon.com was able to stop Barnesandnoble, one of its most significant competitors, from using a similar feature. Nonetheless, there are difficulties in obtaining patent protection. One of the principal is the effort and expense in obtaining one. For one thing, the applicant has to conduct his or her own research into the patentability of the product, which includes discovery of any existing patents in the area. Also, as I have indicated, there are some products which cannot receive patent protection. In the context of computer and information technology, the most relevant distinction is that between a "discovery" and an "invention." The latter is patentable, the former not. For example, a mathematical formula like the Pythagorean theorem, or how to calculate a differential, or something else which is considered a part of nature, cannot receive patent protection. It is necessary to *invent* something, not *find* it.

The example of pharmaceutical companies and indigenous people shows the difficulty in drawing the line between the two. Technology makes the distinction even harder. One example concerns research in biotechnology and the human genetic code. The human genome project (HGP) is a broad-based, international and collaborative effort to produce a map of the entire human genetic sequence. The preliminary results of this project were released in June, 2000. One widely anticipated consequence of the research is the improved treatment of genetically based diseases. At this point, one arrives at a difficulty. Presumably, the treatment involves modifying the genetic code of those who carry the "abnormal" gene to match the code of those who carry the "normal" gene, and, presumably, this information can be derived from studying the results of the genome project. Should such a treatment be patentable? In other words, is it a discovery or an invention? Biotechnology companies strongly argue, because of the research effort involved, and because they will be isolating a given gene from the sequence that contains it, that the resulting treatments will be inventions, subject to patent protections. Hence, when President Clinton and British Prime Minister Tony Blair announced that the

---

[35] "Plaintiff's single-action ordering method addressed an unsolved need that had been long-felt (at least in the relatively short period of time that e-commerce has existed), namely streamlining the on-line ordering process to reduce the high percentage of orders that are begun but never completed, i.e., abandoned shopping carts. The problem of on-line consumers starting but abandoning shopping carts was acknowledged by both parties and their experts …. In the on-line industry in general and at barnesandnoble.com in particular, over half of the shopping carts started by customers are abandoned before checkout …. The single-action ordering invention of the '411 patent solves the problem by eliminating the checkout process entirely" (*Amazon.com*, 1237).

[36] "The Court finds that none of the prior art references offered by Defendants anticipate the claims of the '411 patent. On the question of obviousness, the Court finds that the differences between the prior art references submitted by Defendants and the '411 patent claims are significant. Moreover, there is insufficient evidence in the record regarding a teaching, suggestion, or motivation in the prior art that would lead one of ordinary skill in the art of e-commerce to combine the references. The Court finds particularly telling Dr. Lockwood's admission that it never occurred to him to modify his Web Basket program to enable single-action ordering, despite his testimony that such a modification would be easy to implement. This admission serves to negate Dr. Lockwood's conclusory statements that prior art references teach to one of ordinary skill in the art the invention of the '411 patent." (*Amazon.com*, 1235-1236, citations omitted). The court also cites testimony from amazon.com people on this point. Note that, as this evidence shows, non-obviousness and novelty can be closely related issues.

results of the genome project should be part of the public domain (*i.e.*, implying that they were not patentable), stock in the biotech companies dropped so sharply that the entire NASDAQ exchange fell by 8%. On the other hand, the genetic code seems to be a part of nature: all people carry it. Resolution of this question turns on a number of very difficult issues: to what extent is the genetic code "in nature" versus the extent to which any useful knowledge of it is the product of the application of technology? To what extent can the gene itself be distinguished from the "medicine" it enables? To what extent should society balance the interests of biotechnology companies versus the public interest in knowledge of the human genome? What sort of balance would achieve the best social result – the treatment and elimination of diseases? A poet and waitress from Bristol, England, Donna Rawlinson Maclean, symbolically set all these issues into focus: she applied for a patent for an invention called "myself," explaining that "it has taken thirty years of hard labor for me to discover and invent myself, and now I wish to protect my invention from unauthorized exploitation, genetic or otherwise."[37]

Another question which arises: is a computer program a discovery or an invention? At first glance, a computer program seems rather obviously to be an invention. Most computer programs or routines have utility, most are non-obvious, and many programs are certainly innovative. On the other hand, anything which a computer can do is *by definition* expressible in an algorithm, which means that it can be reduced to a mathematical formula. As a matter of practice, courts have generally ruled that computer programs can be patented, according to the following logic. In *Diamond v. Diehr*, one of three such decisions dealing with the patentability of computer programs, the Supreme Court distinguished between an mathematical formula in the abstract, and its application:

> We recognize, of course, that when a claim recites a mathematical formula (or scientific principle or phenomenon of nature), an inquiry must be made into whether the claim is seeking patent protection for that formula in the abstract. A mathematical formula as such is not accorded the protection of our patent laws, and this principle cannot be circumvented by attempting to limit the use of the formula to a particular technological environment ….On the other hand, when a claim containing a mathematical formula implements or applies that formula in a structure or process which, when considered as a whole, is performing a function which the patent laws were designed to protect (e.g., transforming or reducing an article to a different state or thing), then the claim satisfied the requirements.[38]

One might imagine the distinction by thinking about different kinds of programming languages. As anyone who has ever programmed in a high level language knows, the process of producing a mathematical formula from such a high level program is not without complications. The difficulty in making such a translation suggests the separation between the innovative effort in using the formula – which may be unknown to the programmer – and the formula itself. Or, one might think of a sorting routine: the algorithm for a given

[37] For a brief but thoughtful discussion of some of these issues, see Jeff Howe, "Copyrighting the Book of Life," *Feed* (April 12, 2000), at URL: http://www.feedmag.com/dna/bookoflife.html .

[38] *Diamond v. Diehr*, 450 U.S. at 191-92 (citations omitted and emphasis added).

recursive sort may not be patentable, but its application in a particular search engine might. In the latter case, one can clearly see that the resulting search engine takes the algorithm and produces a useful, nonobvious, innovative product which is contained in the algorithm.

Hence, the distinction is between the algorithm itself and doing some work with the algorithm. As a recent district court decision put it, "as repeated thrice by the Supreme Court and echoed by the Federal Circuit and the C.C.P.A., the best clue to patentability remains the mathematical algorithm/physical transformation test."[39]

Still, one might argue that these decisions are in error, and that extending patent protection to computer programs is a bad idea. For one, the availability of such patents seems to be causing a rapid proliferation of patents in computer software. Some commentators suggest that this proliferation, in addition to risking a logjam, risks ultimately *decreasing* innovation in software development. The more processes and routines that are accorded patent protection, the more work any given programming team has to invent (on its own) in a project simply to reach the status quo of innovation. In other words, excessive patent protection risks creating a situation where good ideas cannot be shared, to the detriment of software development in general, even if to the benefit of some individual developers. This problem: not whether intellectual property rights are desirable, but how many of them, is recurrent.[40]

[39] *State Street Bank v. Signature Financial Group*, 927 F. Supp. 502 (1996), 26. The cited circuit court decision states: "It is first determined whether a mathematical algorithm is recited directly or indirectly in the claim. If so, it is next determined whether the claimed invention as a whole is no more than the algorithm itself; that is, whether the claim is directed to a mathematical algorithm that is not applied to or limited by physical elements or process steps. Such claims are nonstatutory. However, when the mathematical algorithm is applied to one or more elements of an otherwise statutory process claim, the requirements of section 101 are met" *In re Schrader*, 22 F.3d 290, 292 (Fed. Cir. 1994)(quoting *Arrhythmia*, 958 F.2d at 1058).

Trademark

Trademark law is, in general, concerned to protect the name or brand logo associated with a product. If I have a valid trademark to a product, that means that you can't market a similar product with the same (or very similar) name (or logo, or symbol, etc.). Hence, the primary piece of trademark legislation, the Lanham Act, establishes limited monopoly rights for the owner of "any word, name, symbol, or device, or any combination thereof," in order "to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods, even if that source is unknown."[41] The purposes of such legislation were articulated by the Supreme Court in a recent decision as follows:

> In principle, trademark law, by preventing others from copying a source-identifying mark, 'reduce[s] the customer's costs of shopping and making purchasing decisions,' for it quickly and easily assures a potential customer that this item – the item with this mark -- is made by the same producer as other similarly marked items that he or she liked

[40] See Mark A. Haynes, Haynes, "Black Holes of Innovation in the Software Arts," *Berkeley Technology Law Journal* 14:567 (Spring 1999), 567-575; and the theoretical exploration in Michael A. Heller, "The Tragedy of the Anticommons: Property in the Transition from Marx to Markets," *Harvard Law Review* 111 (1998), 621-688. It is also of course possible to argue that there should be no intellectual property rights in software. See Richard Stallman, "Why Software Should not Have Owners," at URL: http://www.draper.net/gnu/philosophy/why-free.html.

[41] 15 U.S.C. §1127

> (or disliked) in the past. At the same time, the law helps assure a producer that it (and not an imitating competitor) will reap the financial, reputation-related rewards associated with a desirable product. The law thereby 'encourage[s] the production of quality products,' and simultaneously discourages those who hope to sell inferior products by capitalizing on a consumer's inability quickly to evaluate the quality of an item offered for sale.[42]

In other words, the goal is to prevent consumers from being confused by similar product marks. In the *Qualitex* decision quoted above, the court emphasized that "it is the source-distinguishing ability of a mark – not its ontological status as color, shape, fragrance, word, or sign – that permits it to serve these basic purposes."[43] Hence, in that decision, the court unanimously held that the green color used by Qualitex for the pads it made for dry-cleaning presses could qualify for trademark protection; Qualitex was therefore able to make a trademark claim against a competitor who made pads of a similar color. Unlike copyright or patent, where the emphasis lies on the product, the emphasis in trademark remains on the symbol, and its capacity to confuse consumers: if the symbol would not cause consumer confusion (for example, restaurants having the same name but in different states, or completely different products of the same name), then both uses can be allowed.[44] There is also a fair use exemption: if my commercial uses your trademark in order to distinguish your product from mine (think of the "taste test" advertisements for soft drinks), that is allowed.

Insofar as the Internet is itself a giant set of linked symbols – words, pictures, logos, etc. – which is available in the same way and at the same time to people regardless of their geographic location, one can expect that numerous problems would emerge in extending trademark law to it. As one commentator notes, "the Internet has also generated many trademark-related controversies, where the difficulty relates to incomplete control of the reputational capital associated with the source of the digitized material, rather than control of the digitized material itself."[45] After all, all Internet sites are, from the point of view of viewers, in the *same* geographic area. One district court judge put the problem quite succinctly:

> The Court is mindful of the difficulty of applying well-established doctrines to what can only be described as an amorphous *situs* of information, anonymous messenger of communication, and seemingly endless stream of commerce. Indeed, the

---

[42] *Qualitex v. Jacobsen Products*, 514 U.S. 159 (1995), 163-164. Internal citations to: 1 J. McCarthy, *McCarthy on Trademarks and Unfair Competition* § 2.01[2], p. 2-3 (3d ed. 1994).

[43] *Qualitex v. Jacobsen*, 164.

[44] "Where two companies each use a different mark and the simultaneous use of those marks does not cause the consuming public to be confused as to who makes what, granting one company exclusive rights over both marks does nothing to further the objectives of the trademark laws; in fact, prohibiting the use of a mark that the public has come to associate with a company would actually contravene the intended purposes of the trademark law by making it more difficult to identify and to distinguish between different brands of goods." *Brookfield v. West Coast Entertainment*, 174 F.3d 1036 (9CA, 1999), 1053.

[45] Dan L. Burk, "Muddy Rules for Cyberspace," *Cardozo Law Review* 21 (1999), 121-179 at 124 n. 19.

> very vastness, and manipulability, of the Internet forms the mainspring of plaintiff's lawsuit.[46]

Although there are many areas of trademark controversy online, one of the main ones involves domain names. Companies want their trademark name plus ".com" to be protectable, because that's how customers look for their websites. An average person, looking for a corporate website, simply tacks ".com" to the corporate name. Hence, a customer looking for "Nike" instinctively searches for "nike.com."[47]

A trademark can be either federally registered or not. A federally registered trademark has been applied for and shown not to conflict with an existing one. Registration then establishes a *prima facie* presumption that the trademark is valid, which is to say that it establishes the presumption that a competing product is not allowed to use a similar mark. The most important way to overcome this presumption is to show "priority of use" – *i.e.*, that you used the mark first.[48] This use has to be *public*. This distinction is an issue for domain names, because getting the name registered and using it publicly may occur at different times, and courts have made use of that distinction. In the *Brookfield* case, of which more below, the court dated a company's use of the trademark from the date it publicly announced the website, which was well after it got the domain name registered.[49] Two case examples will indicate both the difficulties in applying trademark to the Internet, as well as the current confused state of legal precedent.

The first case example is *Brookfield Communications v. West Coast Entertainment.* Brookfield had been making software for searching about movie information and distributing it through retail stores since the late 1980s, and had used the trademark logo "MovieBuff" in its products, including (eventually), a website. West Coast, which is a large video rental chain, launched the moviebuff.com website with a searchable database. Brookfield brought suit, and won at two levels. First, West Coast's use of "MovieBuff" was likely to create actual consumer confusion about the products, and profit from the good name that Brookfield had

---

[46] *Playboy v. Netscape*, 55 F. Supp. 2d 1070 (CD Ca, S. Div., 1999), 1073.

[47] It is an open question the extent to which top-level domain names (.com, .gov, etc.) are involved in this process. The possible confusion is easy to illustrate: if one types "whitehouse.gov," one arrives at the site for the U.S. presidential residence. If one types "whitehouse.com," one arrives at a porn site. If one types "whitehouse.org," one arrives at a "coming soon" message, with the following text appended: "Look for a new and improved Whitehouse site soon. We're just waiting on a few campaign contributions to be wired in from overseas. In the meantime, there's always bondage.com if you're looking for chicks, or userfriendly.org if you're looking for humor." "Whitehouse.net" returns the presidential residence, "whitehouse.de" (Germany) reports being under construction, and "whitehouse.co.uk" (equivalent to .com for Britain) brings one to a digital recording studio (visited June 30, 2000).

[48] "The first to use a mark is deemed the 'senior' user and has the right to enjoin 'junior' users from using confusingly similar marks in the same industry and market or within the senior user's natural zone of expansion" (*Brookfield*, 1047).

[49] "West Coast first announced its web site at 'moviebuff.com' in a public and widespread manner in a press release of November 11, 1998, and thus it is not until at least that date that it first used the 'moviebuff.com' mark for purposes of the Lanham Act. Accordingly, West Coast's argument that it has seniority because it used 'moviebuff.com' before Brookfield used 'MovieBuff' as a service mark fails on its own terms. West Coast's first use date was neither February 1996 when it registered its domain name with Network Solutions as the district court had concluded, nor April 1996 when it first used 'moviebuff.com' in e-mail communications, but rather November 1998 when it first made a widespread and public announcement about the imminent launch of its web site" (*Brookfield*, 1053).

gained from its own products. Second, the use would create "initial interest confusion" – usage of the term in the HTML descriptors would cause people who search for "moviebuff" to generate a list including West Coast, and a certain number of people who looked for the search engine based on their brand recognition of "MovieBuff" would go to the competitor's site instead. Hence, the *Brookfield* decision seems to suggest that trademarked terms can be straightforwardly ported to the Internet.

The second case example, *Playboy v. Netscape*, shows the inherent difficulties in this formulation. Web search engines often sell tailor-made advertising based upon what words you use in your search – the selection of ads which pop up on your screen is determined in part by what you look for. For example, if you look up words that sound like they're looking for cars, you will get banner ads for car products on the results page. Search engines like Excite.com generate revenue by selling advertisers participation in the targeted advertising: every time a targeted advertisement appeared, Excite collected $.05 from the advertiser. In this case, Playboy Enterprises, Inc. (PEI) sued Excite, because "playboy" and "playmate" were on the list of words that generated adult ads, but not specifically for PEI products. Citing *Brookfield*, PEI asserted that these ads diverted people away from the PEI sites which were of superior quality (!) and which were what people were probably looking for anyway. The court rejected Playboy's argument on virtually every count; the one I want to focus on here concerns the status of the words. The court said that the words had common usage beyond the brand recognition and that Playboy couldn't claim protection for these common words.[50] This ruling also makes sense – but it seems difficult to make a principled separation between *Playboy* and *Brookfield*.

Internet searches after these cases bear out the strangeness of the entire issue. As of this writing, typing the word "playboy" into Excite generates a banner ad for the magazine of the same name, several links to Excite directories, and a list of sites. The first is in fact the PEI site; however, of the top 10, most are to other adult sites.[51] A search on Altavista (a different search engine) for "playboy" reported 450,000 results (!).[52] Searching for the phrase "movie buff," rather than the single word "moviebuff" produces an ironic result. That search generated 6,149 results, of which the *first* listed was "WESTCOASTVIDEO.COM: The Movie Buff's Online Movie Store." After all, the phrase "movie buff" is not the same thing as the one-word trademark name, even though the *Brookfield* court indicated that all possible capitalizations of the word were equivalent for the purpose of Internet searches. Searching for the single word "moviebuff" generated 441 pages, of which the first two were Brookfield's "MovieBuff Online." Perhaps not inappropriately, the third linked to a law office's page and was in reference to the court case.

All of this best serves to illustrate the difficulties of adapting trademark to the Internet. In brief: since there is nothing to the Internet other than symbols, and since the Internet is not amenable to any ordinary concept of "place," it is difficult to draw lines between a recognizable product and a similar word (or color, or symbol) etc. The increasing commercial value of the Net can only bring an increase in these sorts of issues. In any case, the courts will be confronted with a balancing test, having to weigh the

[50] "As English words, 'playboy' and 'playmate' cannot be said to suggest sponsorship or endorsement of either the web sites that appear as search results (as in Brookfield) or the banner ads that adorn the search results page. Although the trademark terms and the English language words are undisputedly identical, which, presumably, leads plaintiff to believe that the use of the English words is akin to use of the trademarks, the holder of a trademark may not remove a word from the English language merely by acquiring trademark rights in it," *Playboy vs. Netscape*, 1074.

[51] See http://www.excite.com (visited May 22, 2000).

[52] See http://www.altavista.com (visited May 22, 2000).

private interest of companies in profiting from their use of a symbol, and the public interest in having that symbol freely available in communication.

The Anti-Cybersquatting Act

One of the main problems associated with trademarks and domain names has been the practice known as "cybersquatting." The problem arises because top-level domain names have to be unique. For example, although there can be both a nike.org and a nike.com, there can be only one nike.com. Once a given organization or person has registered that name, it becomes unavailable for anyone else. Since registration is comparatively cheap, it became common practice for "cybersquatters" to register corporate names and the names of famous personalities, such as Nike and Michael Jordan as ".com" sites. When the shoe company and the basketball star tried to register themselves as ".com," they were informed that the name had been taken. The cybersquatters then ransomed the names at considerable profit. In a particularly bizarre instance, Cambridge philosopher Mark Hogarth registered the names of 130 writers such as Jeanette Winterson.[53]

In the United States, this practice was explicitly outlawed by the "Anti-Cybersquatting Consumer Protection Act" of 1999. Since the law is new, there is relatively little commentary on it. The statutory text makes clear what the law is trying to do, however:

The "Anti-Cybersquatting Consumer Protection Act" says the following:

> A person shall be liable in a civil action by the owner of a mark, including a personal name which is protected as a mark under this section, if, without regard to the goods or services of the parties, that person--
>
> (i) has a bad faith intent to profit from that mark, including a personal name which is protected as a mark under this section; and
>
> (ii) registers, traffics in, or uses a domain name that--
>
> (I) in the case of a mark that is distinctive at the time of registration of the domain name, is identical or confusingly similar to that mark;
>
> (II) in the case of a famous mark that is famous at the time of registration of the domain name, is identical or confusingly similar to or dilutive of that mark; or
>
> (III) is a trademark, word, or name protected by reason of section 706 of title 18, United States Code, or section 220506 of title 36, United States Code.[54]

In other words, you can't just register another company's trademark name as your .com name. The "bad faith" part is designed to stop the selling-off of domain names by squatters. There is also a clause that prevents you from registering another person's name as your domain name (a) without their permission and (b) with an intention to profit. This is designed to stop, *e.g.*, somebody from registering

[53] For Winterson's account, see Jeanette Winterson, "My name is my dot-com," *The Times (London)* (March 29, 2000).

[54] Title III of the Intellectual Property and Communications Omnibus Reform Act of 1999 (106 P.L. 113).

themselves as "michaeljordan.com."[55] The passage of the act brought immediate litigation: on the *same day* that the Anti-cybersquatting act was signed into law, the complaint in *Quokka Sports, Inc. v. Cup Int'l Ltd*. was filed.[56] Quokka is the official licensee of the "Americas Cup" (the boat racing one) trademark, and runs the "americascup.org" website. They won a temporary restraining order[57] against the defendant, who runs "americascup.com," on the argument that it would delude people into thinking it was the official site.

Litigation, of course, can be very expensive, and the World Intellectual Property Organization (WIPO), which is part of the United Nations, has set up a dispute resolution procedure which avoids the need for litigation. It also solves questions of jurisdiction, since its results apply internationally. As of June, 2000, WIPO reported that over 600 cases have been filed since December, 1999 when the arbitration system was established; of the 179 cases decided, 147 led to the eviction of the cybersquatter. Jeanette Winterson won back her site, as did Christian Dior, Nike, Deutsche Bank, and Microsoft. Celebrities with pending cases include Tina Turner, the band Jethro Tull, and the estate of Jimi Hendrix.[58]

[55] "Any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, shall be liable in a civil action by such person" (*ibid*.).

[56] No. C-99-5076-DLJ (ND Ca, Dec. 13, 1999).

[57] This is similar to a preliminary injunction: the court tells someone to stop doing something pending a full consideration of the case.

[58] "UN blow to cybersquatters seeking a quick buck," *Reuters* (June 9, 2000).

Copyright

With regards to computers, copyright law is both more developed and more contentious than other areas of intellectual property law. Before outlining the statutory and judicial development of the application of copyright to computers, it is perhaps worth mentioning a couple of conceptual issues underlying the entire debate.

First, copyright (as well as the other IPR's, but the point needs to be underscored here) explicitly serves a utilitarian end. That is, the Constitution says that the purpose of copyright is: "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[59] In this regard, it does not function like "moral rights" or deontological rights, although one might be led to the conclusion that those who have an economic stake in copyrights desire that it does.[60] The question confronting a copyright system, at least in the United States, then, is necessarily about whether that system best achieves the progress of the arts, by balancing the rights of the author, on the one hand, and the rights of the public, on the other. Because the rule is utilitarian, it can be subject to a variety of "policy-oriented" details which serve to refine it and help it to achieve its purpose. Copyright law is, in other words, extremely complicated, and the following discussion will be a substantial simplification.

The rights of the author are addressed by granting the author (or copyright owner, such as a book company or record label) the exclusive right to distribute a given work for a limited period of time. Others who wish to make use of those works must pay the author for the privilege, which he or she can (sometimes) deny. The rights of the public are addressed by the requirement that these

[59] U.S. Constitution, Art. I, §8, Cl. 8.

[60] European interpretations of Copyright, on the other hand, focus on the moral rights of authors.

exclusive rights are granted to the author for only a limited period of time. After that time, the expressions become part of the "public domain," which names the legal space inhabited by works which are owned by nobody in particular. Anyone is free to take and use expressions from the "public domain." For example, it is not necessary to pay a licensing fee to someone in Stratford-upon-Avon for the right to perform a Shakespeare play. The rights of the public are also addressed by a requirement of originality: in order for an author to claim copyright protection, the work must be in some way original to the author. If part of a work is original and part is not, only the part which is original can be given copyright protection. Finally, the rights of the public are addressed by a system of "fair use." According to fair use doctrine, certain activities – such as making a backup copy of a computer program, videotaping a TV broadcast to view later, and copying library articles for the purpose of personal academic research – are allowed, even though they might be thought to violate an author's right to distribute his or her work.

Second, digital technology creates tremendous problems for copyright law because of the tremendous ease with which computers make copies. Regardless of the legal system, one advantage authors held was the difficulty in copying their works. Indeed, copyright was initially invoked against competing publishers, since only publishers had the resources to widely distribute works. Furthermore, successive copies were usually of inferior quality to an original, as anyone who has compared a photocopy made from an original and one made from another photocopy knows. The development of technology has made copying progressively easier, simultaneously reducing the barriers to individuals making copies and increasing the quality of those copies. The combination of computers and the Internet have in turn effected a qualitative change. On the one hand, the fact that WebPages are globally accessible and easily publishable, means that anyone has the capability of achieving a global distribution of any work they put on their WebPages, whether they have a right to copy it or not. On the other hand, digital copying is "noise-free," in the sense that each copy is exactly identical to the "original." In other words, the possessor of an "original" copy of a work has no material advantage over the possessor of a copy of a copy of a copy.

Together, these changes have created a collective terror in the "copyright industry," the umbrella term for the movie, recording, and other publishing industries. The copyright industry reports enormous losses from the unauthorized copying of copyrighted material, and all indications are that this copying will continue. From the point of an individual user, it makes little sense to purchase a copy of a product, when one can have an equally high-quality copy for free. Hence, for example, the *battle royale* over Napster.com, a web service which allows users to share music files with one another. The recording industry has been largely successful in its legal efforts against Napster, but numerous commentators have pointed out, Napster represents the tip of a copying iceberg. Napster relies on a centralized website for its distribution, and so presents a target for legal action. Newer programs, such as "gnutella" operate without such a centralize site and so do not present such an easy target. In a certain sense, to shut down gnutella would require shutting down the entire Net.[61] The response of the copyright industry has been to demand stronger copyright laws, in order to have increased legal resources against such copying. In particular, the copyright industry has sought to disable the technical ease of copying, by lobbying to outlaw programs which break copyright protection schemes, and by lobbying for the enforceability of "shrink-wrap" licenses. The pitch of debate surrounding intellectual property law in general can perhaps best be illustrated by statements of industry spokespeople.

---

[61] For a discussion of such programs, see John Markoff, "Cyberspace Programmers Confront Copyright Laws," *New York Times* (May 10, 2000), A1.

Alan Holmer, president of the Pharmaceutical Research and Manufacturers of America, criticized a plan to relax patent protections for AIDS drugs in poor, developing countries, saying that "we recognize that AIDS is a major problem, but weakening intellectual property rights is not the solution."[62]

In order to unravel these issues, a brief history of copyright law and computers is in order. A few preliminary points will help to clarify this history. One should first recall that IPR's in general are designed to protect a creative *work* – notice the quasi-Lockean basis of the property right. This is important (as will be evident) because of database issues.[63] Second, for copyright, the focus is on the expression of an idea, not the mark of the company (trademark) or an object invented (patent), and infringement focuses on identifying a "striking similarity" between two works. In a manner analogous to the way in which patent law distinguishes discoveries and inventions, copyright depends on distinguishing between an "idea" and the "expression" of an idea, with only the latter being eligible for copyright protection. Third, copyright comes from the constitution, and is statutory. Copyright law is, therefore, what Congress says it is. The courts interpret what congress intended the law to say, and how to apply the law in specific cases, but it's not like (for example) abortion rights or other aspects where certain constitutional freedoms are guaranteed independently of or against the legislature.[64]

Computer programs are explicitly protected by a 1980 revision to the 1976 Copyright Act. As Napster indicates, however, there is more to copyright and computers than software copying, although that was an early focus. Indeed, the very dynamics of the "digital economy" means that intellectual property law in general and copyright in particular will be of increasing importance. On the one hand, their relative importance to the economy in general will increase. If one believes that we are moving to an "information economy," then ownership of new information becomes like ownership of land or factories used to be: the basic measure of wealth. Hence, the legal regimes (IPR's) which establish the rules for such ownership become more and more important, the more of our wealth which gets involved in "information." On the other hand, the likelihood that an issue will involve copyright increases with the increase of digitization. Copyright protects expression "fixed in a tangible medium" – as it turns out, most courts think that *loading it into your computer's memory* is enough. In other words, viewing a webpage on your browser is copying it! This is very different from passing around the same copy of a book. Hence, everything turns on how one understands "fair use." This is a substantial shift from previous applications of copyright, which functioned with a relatively underdetermined understanding of fair use.

The most recent major revision to American copyright law is the *Digital Millennium Copyright Act* (DMCA) of 1998.[65] The DMCA serves two primary purposes. First, it is the implementing legislation for the World Intellectual Property Organization (WIPO) treaty, an international agreement aimed at strengthening and harmonizing intellectual property laws internationally. In other

---

[62] Qt. In "Pharmaceutical firms to slash cost of AIDS drugs for Africa," *CNN.com* (May 11, 2000).

[63] *Cf.* The discussion of *Feist*, below.

[64] To recall, its basis is Art. I, §8, Cl. 8: "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." Notice that patent law is also derived from this clause. That copyright law is wholly statutory and dependent on Congress is stated by the Supreme Court in *Bobbs-Merrill Co. v. Straus*, 210 US 339 (1908).

[65] This is a large and complicated piece of legislation. The best summary of it is probably that provided by the Copyright Office. See "The Digital Millenium Copyright Act of 1998: U.S. Copyright Office Summary" (December, 1998), at URL: http://lcweb.loc.gov/copyright/legislation/dmca.pdf.

words, the DMCA is the law by which the United States becomes a fully party the WIPO.[66] As Senator Biden put the goal, "the WIPO treaties and the implementing legislation will update intellectual property law to deal with the explosion of the Internet and other forms of electronic communications." He adds that "the treaties protect literary and artistic works from digital copying, but do not make it illegal to use the Internet in the normal way."[67] One might perhaps object to Biden's disjunction between copying and normalcy, but the intention is relatively clear. We have already seen one example of the WIPO in its arbitration proceedings for cybersquatting.

The second purpose of the DMCA (and, of course, of the WIPO) is to provide statutory answer to many copyright questions brought on by technology. The DMCA includes, among others, specific provisions permitting backup copying, and prohibiting reverse engineering (with a few exceptions). The reverse engineering provisions have been particularly controversial, because they directly impact the computer industry. The prohibition was favored heavily by the entertainment industries as a way to prohibit programs that broke copy protection schemes. It was opposed by the computer software industry, which pointed out the utility of decompiling and reverse engineering in software design, virus detection, etc. In the resulting compromise, reverse engineering became explicitly banned, except for cases involving specific computer industry requests, such as the development of virus detection and security programs, and efforts to ensure the "interoperability" of programs. Libraries also won a specific exemption for decrypting a work to decide whether or not to purchase it.[68] An amendment was also added for programs designed to stop children from having access to pornography. Senator Ashcroft opined, in support of the provision, that "we should never allow any legislation to move forward that intentionally or unintentionally makes good parenting illegal."[69]

The interoperability provisions are receiving somewhat of a test in a case against DeCSS, a program written by a Norwegian teenager and which decrypts the copy protection coding on DVD's. The Motion Picture Association of America, joined with various other parties, immediately brought suit for violation of the DMCA's ban against reverse engineering. In defense, Johannsen argued that he had written the program to be able to read DVD's on his Linux machine, since all the available DVD players ran on Microsoft Windows-based machines. Hence, he explicitly pointed to the interoperability exemption to the anti-circumvention regulations. On its face, the statute does not provide a clear answer to whether

---

[66] Recall that a treaty, though signed by the executive, is not binding in U.S. law until the Senate passes ratifying legislation. The most famous example of a disjunct between legislative and executive policy on treaties was the Senate's failure to ratify the League of Nations. More recently, the Senate has failed to ratify several arms control treaties to which the President has agreed (e.g. the Comprehensive Test Ban Treaty (CTBT), Chemical Weapons Convention (CWC), and START II).

[67] *Congressional Record* 144:61 (May 14, 1998), S4893-4894.

[68] This compromise is discussed critically in Pamela Samuelson, "Why the Anti-Circumvention Regulations Need Revision," *Communications of the ACM* 42:9 (September, 1999), 17-21.

[69] *Congressional Record* 144:61 (May 14, 1998), S4888. *Cf*. the remarks of Senator Grassley and his explicit invocation of copyright's balancing of interests: "It was important to me that the bill be clarified to ensure that parents are not prohibited from monitoring, or limiting access to, their children in regard to pornography and other indecent material on the Internet. I don't believe anyone wants to restrict parents' rights to take care of their children, or to take away tools that might be helpful for parents to ensure that their kids aren't accessing sites containing pornography. The interests of the copyright owners had to be balanced with the needs of consumers and families. I think that the Committee made a significant improvement to the bill in defense of this important protection for our families" (S4891-2).

programs like DeCSS are legally allowed. Also, of course, from the point of view of ethics, the question of whether they *are* legally allowed does not then address whether they *should* be legally allowed. The MPAA asserted that the case would open the floodgates for illegal copying of DVD movies; the Electronic Frontier Foundation, which supplied attorneys for Johannsen, pointed out that DVD movies were much too long to readily copy, even at high bandwidth speeds. In January, 2000, a judge ordered several websites to remove the program from their servers,[70] following with an opinion in February. In the opinion (which, it should be stressed, is in favor of a restraining order, and is intended to establish the probability of the result, not the result itself), Judge Kaplan offers the following criticism of the interoperability defense:

> First, defendants have offered no evidence to support this assertion.
>
> Second, even assuming that DeCSS runs under Linux, it concededly runs under Windows--a far more widely used operating system--as well. It therefore cannot reasonably be said that DeCSS was developed 'for the sole purpose' of achieving interoperability between Linux and DVD's.
>
> Finally, and most important, the legislative history makes it abundantly clear that Section 1201(f) permits reverse engineering of copyrighted computer programs only and does not authorize circumvention of technological systems that control access to other copyrighted works, such as movies. In consequence, the reverse engineering exception does not apply.[71]

It is debatable whether these reasons survive scrutiny, although they do track the statutory language of the anti-circumvention regulation. The first reason either begs the question or sets a standard that no program could meet, thereby eliminating the exception: how could a programmer prove what the "sole purpose" for writing a program was? The second reason seems to say that the availability of DVD players on Windows constitutes a reason why such players should not be available for Linux users. Apart from making no sense, this pronouncement occurred at the same time that the Department of Justice was prosecuting Microsoft for violating federal anti-trust laws. If the third reason is correct, then the framework of the DMCA would further entrench such proprietary access systems. The third reason also requires further clarification as to what constitutes a "computer program:" to what extent is the DVD version of the movie a computer program?[72]

To make matters more complicated, there are questions of free speech at play: if a computer program constitutes "speech," then it is

[70] "U.S. judge orders DVD hack off Internet sites," *CNN.com* (January 21, 2000).

[71] *Universal City Studios v. Reimerdes*, 82 F. Supp. 2d 211 (SD NY, 2000), 218. Unless noted otherwise, references are to this injunction.

[72] Judge Kaplan freely admits of the difficulties in the case. In one place, for example, he points to "the core issues in the case – the proper construction of the DMCA, which turns on matters including what DeCSS does, what its uses are, and to some extent the motives for defendants' actions, and the DMCA's constitutionality." As of this writing, the defense is involved in a series of extravagant efforts to delay the trial date (including a rather bizarre motion to recuse the judge); these tactics seem to dim the hope that the relevant issues will be adequately considered in this case. The stalling tactics are fully detailed in the denial of recusal, *Universal Cities v. Reimerdes*, 00 Civ. 0277 (LAK) (July 17, 2000). The above passage is from this decision, p. 25.

presumably protected under the First Amendment. The Supreme Court has already ruled that speech on the Internet should receive the highest level of Constitutional protection.[73] *Universal City Studios* does not cite that opinion, but refers instead to a 1925 Supreme Court opinion which established that "freedom of speech is important both as a means to achieve a democratic society and as an end in itself. Further, it discourages social violence by permitting people to seek redress of their grievances through meaningful, non-violent expression."[74] Judge Kaplan asserts that DeCSS does little to achieve these goals, cites favorably the "unquestionably high social value"[75] of a copyright protection scheme which encourages the production of creative works, and concludes that therefore the DeCSS code should not be constitutionally protected speech. Or, it should at least not be protected enough to override these goals.

This reasoning leaves open at least three questions. First, one wonders about the status of program code as speech. Judge Kaplan, in *Universal City Studios*, is fairly dismissive of it as merely functional (and not expressive). On the other hand, the 6th Circuit Court of Appeals ruled in April, 2000 that "the fact that a medium of expression has a functional capacity should not preclude constitutional protection," and that because "computer source code is an expressive means for the exchange of information and ideas about computer programming" it *should* receive constitutional protection.[76] The Court of Appeals does not establish how much protection the code should receive, but it is speaking about encryption code. Second, one wonders how the "end in itself" of free speech is or is not to be weighed against copyright protection for DVD's. Finally, assuming that speech on the Internet is to receive a high level of protection, such protection is traditionally afforded by applying "strict scrutiny" to statutes which restrict speech. To pass "strict scrutiny," a law has to (a) serve a compelling governmental interest, (b) be narrowly tailored to serve that interest, and (c) be the "least intrusive means" available in its achievement. Even assuming that protection of the entertainment industry met (a), the anti-circumvention provisions seem not to be narrowly tailored – as evidenced by the fact that they are an expansive, blanket prohibition, with (particularly as interpreted by this judge), very narrow exceptions. All of which leads one to underline that questions of copyright on the Internet are both difficult to resolve, and require thought about a wide-ranging set of social values and goals, often in the absence of clear legislative or judicial guidelines.

To return to the DMCA, the act makes other clarifications to copyright law. For example, in response to a famous computer piracy case, it codifies that making illegal copies can be criminal copyright infringement even if one does not personally profit from the activity. In this case, David LaMacchia had run a bulletin board, encouraging subscribers to download free copies of copyrighted computer programs. He then successfully defended himself against criminal copyright infringement with the argument that he did not profit from the activity.[77] The DMCA also offered an exemption to Internet service providers (ISP's) from what is known as "contributory infringement." Under copyright statute, it is not only copyright infringement to make unauthorized copies of works; it is infringement to help others do so. This led to a question about the liability of ISP's and bulletin board operators whose subscribers upload pirated games and programs? The DMCA included a general exemption for such ISP's, provided (more or less) that they were ignorant of the activity at the time it happened, and had taken efforts to stop it once they learned of it.

---

[73] *Reno v. ACLU*, 521 U.S. 844 (1997).
[74] *Universal City Studios*, 221-222.
[75] *Universal City Studios*, 222.
[76] *Junger v. Daley*, 209 F.3d 481 (6CA 2000), 484-485.

[77] *U.S. v. LaMacchia*, 871 F. Supp. 535 (USD Mass, 1994).

In general, the DMCA was substantial piece of compromise legislation which enjoyed broad-based, bipartisan support. Whatever one does or does not like about its details, it seems important to recognize that it represents a first comprehensive attempt by Congress to deal with the complexities of copyright and the digital economy. Senator Ashcroft modestly concluded: "in the end, this is not a perfect bill. I would have favored a different approach to some issues. However, this bill is an important step forward in bringing the copyright law into the digital age."[78] Particular controversy continues in two primary areas: (a) is a given material copyrightable? And (b) is the use of it "fair"? The controversies surrounding the latter are particularly fueled by computer industry opposition to, and entertainment industry support of, the anti-circumvention regulations.[79]

The question as to whether material is copyrightable is not as easy to answer as might first appear, since it is sometimes difficult to measure the originality of the expression of a program. What, after all, besides the name, is the difference between the Microsoft Office and Corel Office Suite products? The following three court cases will serve to illustrate some of the issues involved.

In the first case, *Apple v. Franklin*, Franklin Computers copied (and freely admitted so doing) the code for the Apple II operating system.[80] Franklin offered two basic defenses (a) "the use of identical signals was necessary in order to ensure one hundred percent compatibility with application programs created to run on the Apple computer" (1245). In other words, copying was necessary to ensure interoperability; the applications were the focus. (b) The operating system could not be copyrighted, for several reasons. The most important was that it was not an application, and therefore more like the hardware of the machine than the software applications for it. Franklin also argued that the source and object codes were different in terms of copyright protection. The court rejected all of Franklin's arguments, holding that operating systems could be copyrighted, because they were also application programs and that the fact that source code had to be translated into object code did not mean that the object code was part of a different program – any more than (this is my example) the fact that the music on a CD is digitized means it's different music.

The second case is *Whelan v. Jaslow* (1985).[81] This case was complicated by a series of contracts between the parties. The most important holding was that the court defined the "expression of the idea" of a computer program as something which was not dependant on the computer language it was written in. The court emphasized two factors in determining whether programs were the same or sufficiently similar expressions: (a) expert testimony (1321) and analysis. Whelan produced experts who showed that Jaslow pretty obviously copied the program, and could not have come up with the program on their own;[82] and (b) the visual similarity between the programs. Jaslow's program *looked* and ran identically to Whelan's, even though the languages were different.[83] One should also draw from *Whelan* a note about the costs of litigation: Whelan won about $200k in damages, but had to pay $188k in attorney's fees – which the court did not award because of the novelty of the case.

The final case, *Feist v. Rural Telephone*, was unanimously decided by the Supreme Court in 1991.[84] The first two cases expand

[78] *Congressional Record* 144:61 (May 14, 1998), S4891.
[79] For further discussion, see "Cyberspace Programmers Confront Copyright Laws," *New York Times* (May 10, 2000), A1; and "Battle Brews over Reverse Engineering," *CNN.com* (May 8, 2000).
[80] *Apple v. Franklin*, 714 F 2d 1940 (3CA 1983).
[81] *Whelan Associates v. Jaslow Dental Laboratory, Inc.*, 609 F.Supp. 1307 (EDPa 1985), affirmed 797 F.2d (3CA 1986).
[82] *Whelan v. Jaslow*, 1321.
[83] *Whelan v. Jaslow*, 1322.
[84] 499 US 340 (1991).

what can be protected. This one limits it. Feist copied about 1200 phone numbers from Rural's white pages in constructing a regional telephone directory; Rural sued for Copyright infringement. The Court held that facts cannot be copyrighted – the key to copyright protection is "originality," and *not* the "sweat of the brow." In other words, it does not matter how hard one works – one has to have done something at least minimally original to be awarded copyright protection for one's labors. To be protected, a compilation of facts needs "an original selection or arrangement" (348), and that copyright extends only "to those components of a work that are original to the author" (348).[85] The Court then declared:

> There is nothing remotely creative about arranging names alphabetically in a white pages directory. It is an age-old practice, firmly rooted in tradition and so commonplace that it has come to be expected as a matter of course (363).

This decision has created alarm in the database industry. As the Internet and computer technology in general makes more and more information "available" in the sense of existing in a form that can be compiled and searched or "mined," a substantial and profitable trade has emerged in such database compilation programs. *Feist* seems to deny legal protection to such databases. In response, the database industry has proposed a *sui generis* (of its own type) protection for computer databases, which the Europeans are considering, but which seems unlikely to pass here, at least at the moment.

---

[85] In this case, the preface, etc. to the phone book, but not the numbers themselves or their alphabetical arrangement.

CHAPTER IV: PRIVACY

It is somewhat of a commonplace to worry about the effects of technology on "privacy." Indeed, one is tempted to suggest a one sentence version of this chapter: "you don't have any." Numerous articles, books, commentaries and discussions, both popular and scholarly, discuss the extent to which traditional protections of privacy are eroded by computer technology. More to the point (although this distinction is sometimes lost), they are eroded by the combination of computer technology and the way in what that technology is used. The technological source of the problem is easy to identify: computers make it possible to obtain and correlate an unprecedented amount of information about individuals. Increasingly, individuals are "represented" or "profiled" in cyberspace by a cyberpersona; this cyberpersona is an increasingly complete representation of the real individual beneath it. Once a person can be understood by a collection of profiled information, it becomes possible to search, collate, and manage that information for a variety of purposes. Among them is the identification of "risk:" a person whose profile indicates that he or she is statistically likely (for example) to commit a crime is subject to increased surveillance. In this sense, computers enable proactive monitoring of individual behaviors, whether in the form of police surveillance or of insurance companies' premium-setting policies.

This sort of profiling, and this "invasion of privacy" occurs at both government and corporate levels. On the side of government, a fear of computer (and other crime) pushes proposals for intrusive monitoring of electronic communications. On the side of corporations, the drive for efficient profit-making pushes proposals for risk management and tailored advertising. For example, the Internet advertising service DoubleClick proposed to aggregate consumer demographic data with profiles of consumer shopping patterns. This would enable advertisers to indicate not just what a web-persona did, but who the real person underneath that persona was. Only widespread public outcry caused DoubleClick to abandon the policy, but one can be sure that other corporations will attempt similar policies.

Before undertaking a more conceptual look at privacy, some concrete examples, from both government and corporate use of personal information will serve to illustrate the extent to which technology enables this "invasion of privacy."[1] Law enforcement is using technology to proactively track and target certain suspect groups of individuals – rather than reactively trying to solve a crime after the fact. This process is known as red-lining, and it doesn't take much imagination to think of ways it could be abused along racial or class lines. This is an updated version of profiling, where people who looked a certain way would be more likely to be searched at airports. Red-lining enables profiling at an unprecedented level.[2] Surveillance technology now allows tiny, rapidly recording cameras to identify uniquely every vehicle which passes through a certain area, and then to track that vehicle as it drives around a city. Similar technology is available, or soon will be, to individually identify people in a crowd, *e.g.*, of protesters.[3]

---

[1] The first three of these are taken from "An Appraisal of the Technologies of Political Control" STOA Interim Study, Sept. 1998, http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm.

[2] The STOA report summarized its findings on : "the global surveillance systems which facilitate the mass supervision of all telecommunications including telephone, email and fax transmissions of private citizens, politicians, trade unionists and companies alike. There has been a political shift in targeting in recent years. Instead of investigating crime (which is reactive) law enforcement agencies are increasingly tracking certain social classes and races of people living in red-lined areas before crime is committed - a form of pre-emptive policing deemed data-veillance which is based on military models of gathering huge quantities of low grade intelligence."

[3] The globalization of the economy means that such technology can be diffused easily. As the STOA report put it: "Such surveillance systems

The mostly unregulated (and unregulable, under current understandings of executive privilege) National Security Agency (NSA, which is part of the executive branch) "project ECHELON" apparently routinely intercepts enormous amounts of electronically transmitted information (email, faxes, etc.), searches for certain "suspect words" and targets individuals who use those words for further surveillance.[4] This surveillance occurs of private citizens, businesses, as well as groups such as Amnesty International and Christian Aid.

At the corporate level, a number of web sites will sell you, for about $50 a go, information on people such as their social security number, bank balance, credit history, bank account numbers, unlisted phone numbers, addresses, etc. All of this is legal, both for it to be bought (you might have to pretend to be a private investigator) and sold.[5] A couple of examples of specific impacts of this procedure will illustrate the problem. A cyberstalker paid $45 for the social security number of a certain Amy Boyer. He then used the information to find out where she worked, and then killed both her and himself at her workplace.[6] An increasingly common phenomenon is known as identity theft: given your name and social security number, somebody can open false credit cards, etc, in your name, and ruin your credit. Estimates are that 400,000 Americans will face this problem in the year 2000 alone.[7]

These are examples of illegal use of information, or the use of information for illegal purposes. Information can also be legally used for disturbing purposes. For example, recent court decisions make it clear that employees have no expectation of privacy in their emails sent on company computers. Virtually any reading of these emails by the employers is permitted, including automatic monitoring.[8] Pending regulations seem to establish, at least on one reading, that a person's medical records will be available for disclosure as a matter of presumption; individuals will not have control over the usage of their own medical record information. As an EFF position paper put it, "by facilitating disclosure in these many cases, the fact that medical records are profoundly sensitive documents affecting life choices of individuals -- including whether

---

raise significant issues of accountability, particularly when transferred to authoritarian regimes. The cameras used in Tiananmen Square were sold as advanced traffic control systems by Siemens Plessey. Yet after the 1989 massacre of students, there followed a witch hunt when the authorities tortured and interrogated thousands in an effort to ferret out the subversives. The Scoot surveillance system with USA made Pelco cameras were used to faithfully record the protests. The images were repeatedly broadcast over Chinese television offering a reward for information, with the result that nearly all the transgressors were identified. Again democratic accountability is only the criterion which distinguishes a modern traffic control system from an advanced dissident capture technology. Foreign companies are exporting traffic control systems to Lhasa in Tibet, yet Lhasa does not as yet have any traffic control problems. The problem here may be a culpable lack of imagination" (§2.2).

[4] An aspect of the privacy discussion, which falls outside the scope of this chapter, is that of "executive privacy." According to some commentators, one consequence of the Nixon decisions was the creation of an autonomous space of constitutionally recognized executive privilege on areas of "national security." These "private" areas then become outside of "public" control.

[5] "We Know Everything about You," *PC World Online*, Jan. 2000.

[6] *Ibid*.

[7] As one commentator put it, the possibilities of such usage of SSN's provides the "makings of a disaster that makes the recent Y2K computer problem pale in comparison" (Hal Berghel, "Identity Theft, Social Security Numbers, and the Web," *Communications of the ACM*, Feb. 2000, 17).

[8] See Berghel, 19.

to have children, availability of employment opportunities and health treatment options -- is ignored."[9]

Finally, most web sites don't even post their privacy policy – or even have one. As recent examples involving Realmusic and DoubleClick indicate, most have no qualms about collecting and disseminating customers' personal information.[10] Until the Summer of 2000, the Federal Trade Commission (FTC) had supported industry calls for "self-regulation." In other words, industry would figure out on its own how to protect the privacy of consumers. It is not hard to see what this approach was unlikely to generate satisfactory results: after all, there is absolutely *no* economic incentive to protect consumers' privacy, except for perhaps public outcry. However, surveys indicate that most consumers do not know the extent to which their information is compromised, and in any case, as long as no alternative exists to the loss of privacy, consumers have no real choice but to accede to its loss. The situation has become sufficiently dire that the FTC's May, 2000 report calls for legislative enforcement of on-line privacy standards.[11] Indeed, substantial legislation has been introduced (though little has passed) in both federal and state legislatures to address this problem.[12]

Information technology can be tremendously empowering. As these concerns with privacy indicate, it can also be disempowering to individuals. As one commentator put it, "new information technologies are two-sided. They enable and empower, but they make their users more vulnerable to surveillance and manipulation. The two sides cannot be separated: it is precisely

---

[9] See http://www.eff.org/pub/Privacy/Medical/20000216_eff_dhhs_medpriv_comments.html. The EFF suggests that the following scenario would be possible under these regulations as well: "the rule could permit doctors to collect DNA evidence in the course of their treatment. Police could use the good faith exception to obtain the DNA evidence. For example, law enforcement could collect, without a proper warrant, the DNA of anyone recently admitted to the hospital that may have been in a particular area at a particular time. The area and time information would be supplied by the directory and the admittance information kept in the patient's file. In fact, since this information would be kept in a new federal database whose creation is authorized by this rule, the police may not even be required to obtain permission from the doctor." For a critique of the trend toward disclosure, see Amitai Etzioni, *The Limits of Privacy*, 139-182.

[10] *Cf*: "The Internet industry wants the government to refrain from introducing online privacy legislation, yet statistics show that the industry's self-regulation efforts are faring poorly. Indeed, a soon-to-be-released survey by Enonymous.com finds that not even 23 percent of 29,000 Web sites examined post privacy policies on their sites. And most of the policies posted by the sites are paper tigers, according to the survey. Forrester Research says the industry's failure to develop consumer trust is keeping millions of people from shopping on the Internet. A number of recent privacy invasions by high-profile Web sites emphasize this point. The Enonymous.com survey graded Internet companies' privacy policies on a scale of zero to four stars. More than three of every four sites did not receive a star because they did not post a privacy policy. Nearly 8 percent earned one star for failing to give consumers privacy rights. Close to 9 percent of the sites received two stars, indicating that a site will share users' personal data only after receiving users' consent, while three stars were given to 2.7 percent of the sites, meaning that, in addition, the sites will not contact users without their permission. Four stars were awarded to 3.5 percent of Web sites, which extended full privacy protections to consumers. America Online was the only major Web site to receive four stars, while MSN, Yahoo!, and eBay were awarded one." "Web Firms Have Sorry Record on Public's Privacy," *Los Angeles Times* (03/20/00), C1.

[11] *Privacy Online: Fair Information Practices in the Electronic Marketplace*, Federal Trade Commission (May 25, 2000), at URL: http://www.ftc.gov/os/2000/05/testimonyprivacy.htm.

[12] "Dot-coms wary of privacy Bills," *Computerworld Online*, 3/13/00, at URL: http://www.computerworld.com/home/print.nsf/all/000313F692.

what empowers that also extends vulnerability."[13] Privacy thus becomes a value which is brought into question by the development of information technology: just as the ability to collect vast amounts of information about people furthers research on disease prevention, so too the very fact of the information's being collected entails a challenge to the privacy of individuals.

Where does this dilemma come from? "Panopticism" and other ideas

A common metaphor in discussions of privacy and technology argues from the position that, as one commentator put it, "information technology is fast becoming … a virtual panopticon such as even Jeremy Bentham would not have been able to visualize in his wildest dreams."[14] To understand this metaphor, then, we need to understand who Jeremy Bentham was, and what his "panopticon" was.

Bentham was an English legal theorist and philosopher of the early 1800s. As indicated in the chapter on philosophical ethics, Bentham was also basically the founder of utilitarianism. One of his ideas was about developing a new kind of prison, which he called the "panopticon." The basic idea was that prisoners could always be seen by the guards, but that the guards could not be seen by the prisoners, and the prisoners could not see each other. Hence, each prisoner felt that he or she was under the constant supervision of someone: "by *blinds* and other contrivances, the keeper concealed from the observation of the prisoners, unless where he thinks it fit to who himself: hence, on their part, the sentiment of an invisible omnipresence."[15] The panoptic prison would be shaped somewhat like a bicycle wheel: the center would be a guard tower, and the cells would be arranged around it in a circle facing inward, so that a single central tower could see all of the cells at once. This idea became enormously influential in penal theory, even though Bentham's panopticon was never built. The point, in short, is that the total surveillance of prisoners is seen as sufficient to prevent their misbehavior, even without as many guards. The panopticon thus achieves a certain efficiency in imprisonment, and a reduction in the apparent violence of a system based on physical intimidation.

What does any of this have to do with computers and ethics? In contemporary usage, the term "panoptic" usually refers to or is based on the work of the French philosopher Michel Foucault, who used the panopticon as a metaphor to understand how power functions in contemporary society. In his influential *Discipline and Punish*, Foucault observed that society has seen a change in the way punishment was administered. According to Foucault, in medieval and renaissance practice, punishment was inflicted upon the body of the prisoner in a graphic spectacle of torture. In contemporary theory, however, power functions without this overt violence by "disciplining" its subjects. As Foucault puts it, in terms which should indicate the relevance to computer data collection:

> For a long time ordinary individuality – the everyday individuality of everybody – remained below the threshold of description. To be looked at, observed, described in detail, followed from day to day by an uninterrupted writing was a privilege. The chronicle of a man, the account of his life, his

[13] Reg Whitaker, *The End of Privacy: How Total Surveillance is Becoming a Reality* (New York: The New Press, 1999), 101.

[14] Lucas D. Introna, "Privacy and the Computer: Why We Need Privacy n the Information Industry," *Metaphilosophy* (1997), 260.

[15] "Panopticon Papers," in *A Bentham Reader*, ed. Mary Peter Mack (New York: Pegasus, 1969), 194.

> historiography, written as he lived out his life formed part of the rituals of his power. The disciplinary methods reversed this relation, lowered the threshold of describable individuality and made of this description a means of control and a method of domination. It is no longer a monument for future memory, but a document for possible use.[16]

As the example of the prison suggests, the innovation of the panopticon, and hence, of what Foucault calls disciplinary power, is that the prisoner "becomes the principle of his own subjection" (203). Rather than being a body which is repressed by the spectacular assault of the monarch, the criminal has become a "delinquent:" someone whose behavior can be studied, and with the appropriate behavioral techniques of reward, punishment, and education, modified so as to fit the rules of society. Hence, "it is not that the beautiful totality of the individual is amputated, repressed altered by our social order, it is rather that the individual is carefully fabricated in it, according to a whole technique of forces and bodies" (217). Discipline, in this sense, is a form of individuation: one is formed *as* an individual by disciplining oneself to fit the rules of society. Foucault's suggestion is that the panoptic metaphor, originally confined to the prison, has become a model for the organization of all society: "is it surprising that prisons resemble factories, schools, barracks, hospitals, which all resemble prisons"(228)?

One key to the functioning of disciplinary power is the collection of information. If the decision to commit a crime can be understood to be influenced by a series of factors antecedent to it, then one way to reduce crime would be to understand and eliminate those factors. If, for example, it could be discovered that most of those who commit murder have purchased red shoes, then one might suggest either that red shoe purchases be disallowed, or that those who purchase red shoes be subject to increased police surveillance. In order to be able to make such causal generalizations, however, it is necessary to accumulate a vast amount of information about the behavioral patterns of people. It is the ability to accumulate and manipulate information on an unprecedented scale that links computers to thinking about disciplinary power and enables the thought that information technology enables a "virtual panopticon."

There are at least two ways that such linkage can be made. First, The decentralization of the Internet means that every "place" is functionally adjacent to every other place, or easily accessible from every other place (after all, you just type in the URL…). Absent specific defensive measures, one's Internet behavior is always and by default "on display" because that behavior is always immediately or directly visible. There is no normal functional equivalent to hiding behind a hill. In this sense, the architecture of the Internet creates the equivalent of a panopticon. Second, a computer can easily record everything you do on it, down to the last mouse movement or keystroke. This means that one leaves an almost infinitely detailed picture of oneself every time one goes online. One thinks of the convenience store robbers who wore trendy flashing red lights on the heels of their shoes. Running into the woods did not assist their escape from police. The combination of Internet visibility and recording technology creates the equivalent of such flashing red lights for everyone online, all the time. As one commentator suggested, "imagine a complex crisscrossing network of roving searchlights constantly lighting up individuals, who flare momentarily like fireflies, then disappear, only to be lit up again and again."[17]

---

[16] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan (New York: Vintage Books, 1977), 191.

[17] Whitaker, *End of Privacy*, 140.

The more society uses computers, the more normal this situation will become, and the more unavoidable it will become. Arguments that one can "choose" to have privacy by avoiding having data collected, become incoherent. One would not only have to forego all activity online and all credit card purchases and all banking in general. One would have to avoid medical treatment altogether: although one signs a "consent" form to agree to the disclosure of one's medical information, this "consent" hardly indicates choice. Not only is signing it necessary to receive medical care or health insurance, the forms write the equivalent of a blank check, imposing "no limits on what is to be disclosed or to whom, or on the release of personal health information to third parties or the sale of such information to all comers."[18]

Privacy, then, although it is hard to define precisely, names in this context a principle suggesting a limit to such surveillance activities. Privacy says: "off limits – you cannot look here." In this sense, privacy is a "negative" right, imposing a limit on what others cannot do, rather than empowering one to do something. Legal scholar Amitai Etzioni suggests that in most people's minds, privacy manages to be a confused combination of two separate principles. On the one hand, there is the principle that some activities should be outside the realm of social scrutiny – with the implication that they should be tolerated even if or even though most people find them offensive. On the other hand, there is the notion that some activities, which are not only tolerated but encouraged, should be conducted outside of scrutiny.[19] For example, shopping is a socially condoned activity – privacy advocates wish to be able do it without surveillance. Still, one might ask for what one is shopping: is shopping for pornography socially condoned? What about violent pornography? What about shopping for a mail order bride?[20] To take another example, terrorism is something which is not socially condoned. Hence, law enforcement is concerned that privacy illegitimately hides the activities of terrorists. I do not wish to engage in further development of this point here; rather, it seems important to acknowledge that the general concept of privacy is one that is difficult to pin down, and that what one means by privacy will partly determine the extent to which one thinks it should be protected.

Two principal and related ways that privacy advocates seek the protection of privacy online are encryption and anonymity. If surveillance functions by individuating people – allowing one to see who someone is and what they are doing – encryption and anonymity function by severing the link between these two. Encryption means that although someone knows who is speaking, they cannot understand what that person is saying. When data is coded with such "strong encryption," it is unreadable to those who do not have the keys. The debate over encryption seems to revolve around two points. On the one hand, encryption technology will very soon develop to the point that, even if a coded message could, in principle, be cracked, doing so will take so long as not to be worth the effort.[21] On the other hand, the widespread diffusion of encryption technology raises the possibility of communication which is truly outside the possible space of law enforcement. Hence, for the first time ever, even a warranted, legitimate search of

[18] Etzioni, *Limits of Privacy*, 156.
[19] Etzioni, *Limits of Privacy*, 196-197.

[20] See the following chapter on "crime."
[21] The "not worth the effort" clause is important: as several commentators have pointed out, the mere fact that humans have to encrypt data makes it impossible to rely on encryption absolutely. Bruce Schneier, for example, suggests that "cryptanalysts will forever be pushing the envelopes of attacks …. Security must be designed-in from the beginning," rather than added through *post hoc* encryption. See his "Risks of Relying on Cryptography," *Communications of the ACM* 42:10 (October, 1999), 144.

someone's activities and records might, in principle, yield no useful information. This possibility alarms governments, from that of the United States, which fears terrorism, to the totalitarian government of Burma, which fears dissidents. Both sets of fears are warranted. Etzioni, citing a study by Dorothy Denning and Kenneth Baugh, reports that:

> Members of the Aum Shinri Kyo (Supreme Truth) cult, which launched a deadly nerve gas attack on the Tokyo subway in 1995, encrypted computer files that contained details about their plans to inflict mass destruction in the United States. Ramszi Yousef, who was a member of the international terrorist group responsible for bombing the World Trade Center and a Manila airliner, encrypted files on his laptop computer pertaining to additional plans to blow up eleven U.S.-owned commercial airliners in the Far East. After the bombing of the U.S. embassies in Kenya and Tanzania in 1998 it was revealed that the CIA had foiled three other attacks in 1997 by using electronic interceptions. These would not have been possible if the terrorists had used strong encryption.[22]

On the other hand, Phil Zimmerman, the developer of the encryption protocol PGP ("Pretty Good Privacy") reports that pro-democracy activists in Burma used his protocol to protect their address and contact lists – thereby probably saving a number of lives.[23]

Depending on one's point of view, one will see encryption as either a good thing or a bad thing. From the point of view of businesses with trade secrets which need to be protected, encryption is good. It is also good from the point of view of governments planning military operations. Finally, it is good from the point of view of those who write programs which encrypt and decrypt data, for which there is a strong and growing worldwide market. As noted above, from the point of view of law enforcement in particular, encryption is a potential nightmare.

Anonymity functions not by making it impossible to know what is being said, but by making it impossible to know who says it. If one only knows that a certain amount of money is spent online on pornography, rather than who spends it, one is unable to send advertising to people's mailboxes. From the point of view of commerce, anonymity is an unfortunate limitation to data collection, because it makes it impossible to fully determine an individual's patterns of activity. An individual whose activities cannot be fully determined is a potential waste of resources. Not only might potentially interested customers not receive information about products in which they might be interested, irrelevant advertising might be sent to those people. Legal theorist Lawrence Lessig points out, tongue in cheek, that "I do not know why Nike thinks I am a good person to tell about their latest sneakers …. I would love it if Nike knew enough to leave me alone. And if these data were better collected and sorted, it would."[24] Nike would also prefer not to waste money on someone who is simply not going to purchase their products. Another scholar puts it:

---

[22] Etzioni, *Limits of Privacy*, 78.

[23] See, in general, Charles Platt, *Anarchy Online* (New York: Harper Prism, 1996).

[24] Lessig, *Code and Other Laws of Cyberspace*, 152.

> What if one's purchases are carefully recorded to construct a profile of consumption preferences for the use of various marketers? Not everyone will object to this if they see their needs and desires being better served as a result. Think of it as a Christmas wish list that enables Santa to serve you better. The consumer Panopticon rewards participation.[25]

The lack of anonymity, from this perspective, is very much a double-edged sword.

Anonymity concerns are also raised in the context of intellectual property law by the acceptance of shrink-wrap licenses. If these licenses become sufficiently accepted, then one can imagine a state of affairs where no one ever "simply" browses a magazine shelf or bookcase any more. Rather, one discloses a substantial amount of information about oneself – one's reading patterns, for example – prior to even looking at a work. It is easy to imagine that one would not want a detailed record of what one reads. This concern does not just apply to those who hold controversial political views. Although, as the next chapter will make clear, I am opposed to the institution of mail-order brides, research for that chapter included visiting sites advertising just such brides. No doubt, someone or some computer somewhere has now added to my profile the idea not just that I visit mail-order bride sites, but also that I am the sort of person who meets the profile of a typical such visitor. As we shall see, the correction of inaccurate information is an important concern in privacy debates. Here, however, one should note the extent to which the loss of anonymity involves principles at the very heart of free expression. Julie E. Cohen suggests:

> All speech responds to prior speech of some sort. The person who expresses vigorous disapproval of Hillary Clinton after months of reading electronic bulletins on "femi-nazis" from Rush Limbaugh and subscribing to anti-feminist Usenet newsgroups is no different in this regard than the person who reads a judicious mixture of New York Times op-ed pieces and scholarly literature on feminism before venturing to express an opinion regarding Mrs. Clinton's conduct. When the two readers choose to express their own views, the First Amendment protects both speakers equally. Logically, that zone of protection should encompass the entire series of intellectual transactions through which they formed the opinions they ultimately chose to express. Any less protection would chill inquiry, and as a result, public discourse, concerning politically and socially controversial issues -- precisely those areas where vigorous public debate is most needed, and most sacrosanct.[26]

Cohen then goes on to argue that individuals ought to have a right to disable such copyright management technology in order to retain this right to read anonymously. She is speaking of the provisions that became the DMCA's anti-circumvention regulations. From this, one should note the interconnectedness of issues computers and policy – and also the extent to which those issues implicate central social and political values.

---

[25] Whitaker, *End of Privacy*, 141.

[26] Julie E. Cohen, "A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace," *Connecticut Law Review* 28 (Summer, 1996), 1006.

Privacy as a concept

I have already suggested that a precise definition of privacy is difficult to formulate, primarily because people use the word in a variety of ways. In the American legal context, privacy has had somewhat of an uneven development. First, the word does not occur in the Constitution; philosophical scholarship about "privacy" did not really develop until the late 1960's.[27] Hence, the history privacy as a concept is a relatively recent and underdeveloped one, and has less of the nuance that considerations of property sometimes have. Legally, privacy can be protected through either constitutional or statute law. The latter can best be described as a piecemeal hodgepodge of legislation designed to stop specific privacy abuses.[28] Nonetheless, many of these statutes model the 1974 Privacy Act's modeling of the 1973 "Code of Fair Information Practices." This code was developed as an advisory opinion by the Secretary of Health, Education and Welfare's Advisory Committee on Automated Personal Data Systems. The code does not have legal status, though it exists as a model for legislation. It contains the following principles:

> 1. There must be no personal data record-keeping system whose very existence is secret.
>
> 2. There must be a way for an individual to find out what information about him or her is in a record and how it is used.
>
> 3. There must be a way for an individual to prevent information about him or her that was obtained for one purpose from being used or made available for other purposes without his or her consent.
>
> 4. There must be a way for an individual to correct or amend a record of identifiable information about him or her.
>
> 5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of data.

As one might imagine, these rather vague principles have generated a great deal of enthusiasm and very little legislative action. As I suggested, there is little institutional incentive to follow these guidelines. Most of the guidelines suggest individual empowerment as a solution. However, experience with systems established along these guidelines – *e.g.*, that one be allowed to correct a faulty credit record – suggests that such empowerment is entirely chimerical. Reports abound of people whose lives were destroyed before they discovered an error or who found institutions unwilling to correct an error. To the extent that a given piece of incorrect information may have found its way into numerous other databases, and to the extent

---

[27] See Introna, "Privacy and the Computer," 261ff.

[28] Even specific statutory protections are sometimes difficult to understand. For example, the Electronic Communications Privacy Act (ECPA) sets court order requirements for law enforcement officers obtaining evidence from ISP's. At least one court, however, has ruled that evidence obtained in violation of this law need not be suppressed (thrown out). See *U.S. v. Kennedy*, 81 F. Supp. 2d 1103 (USD Kansas, 2000) at 1110. For a survey discussion of the statutory and case law on informational privacy and recommendation for federal legislation modeled on the Code of Fair Information Practices, see Susan E. Gindin, "Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet," *San Diego Law Review* 37 (1997), 1153-1223.

that the path of such information transfers cannot be traced, it becomes practically impossible to correct false information. The other imperatives provide few policy guidelines. As Etzioni suggests about the information contained in medical records, either the use for which someone has given consent will be too broad to protect privacy ("the common good"), or too narrow to allow medical research ("only for this treatment").[29] The current legislative environment does not promise much improvement.

There is a somewhat clear trajectory of judicial enforcement of privacy rights. The notion was originally developed in a famous law review article by Warren and Brandeis in 1890 which concerned newspaper intrusions into their private lives.[30] The first major Supreme Court opinion affirming a constitutional right to privacy was the 1965 *Griswold v. Connecticut*, which basically affirmed that one could find a "zone of privacy" in the "penumbra" of the constitution. This penumbral right was sufficient to invalidate a Connecticut statute forbidding the use of contraceptives by married couples. As the court said, "Would we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship."[31] Since *Griswold*, the privacy right was expanded by the court through the 1960's and 1970's to invalidate restrictions on contraception for unmarried couples;[32] to increase the expectation of privacy of an individual in his her home, as opposed to in a more public space;[33] and to invalidate state bans on abortion.[34] In the mid- to late 1980's, the Rhenquist Court substantially curtailed the scope of privacy rights, most significantly in a series of decisions upholding various restrictions on the abortion right (a ban on state funding, requiring parental notification by minors, etc.) and, in *Bowers v. Hardwick*, upholding a Georgia statute banning consensual adult sodomy.

In this context, *Bowers v Hardwick* is particularly illuminating, because the court basically expressed its discomfort with homosexuality, rather than arguing from any legal principle.[35] For example, Chief Justice Burger, in his concurring opinion, explicitly said that "condemnation of those practices is firmly rooted in Judeao-Christian moral and ethical standards" and that "to hold that the act of homosexual sodomy is somehow protected as a fundamental right would be to cast aside millennia of moral teaching" (196). The example is illustrative because most people have an opinion about it, and that the range of opinions which people express illustrate (a) that privacy marks a contested limit of the extent to which certain social values can legislate individual behavior; (b) that understandings of privacy are context dependent – on the society and what it says is permissible; and (c) that privacy cannot be thought in absolute terms – no one is *absolutely* free from society. In other words, if most people conflate two different concepts – that of legitimate activity carried out without surveillance, and that of activity which should be permitted despite mores against it – this is not without reason. The cases concerning sexual privacy illustrate the complexity of the competing values involved. The observation that privacy is not absolute is of course

[29] Etzioni, *Limits of Privacy*, 177-178.
[30] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4:5 (1890), 193-220.
[31] *Griswold v. Connecticut*, 381 US 479 (1965), 485-486.
[32] *Eisenstadt v. Baird*, 405 U.S. 438 (1972).
[33] *Stanley v. Georgia*, 394 U.S. 557 (1969).
[34] *Roe v. Wade*, 410 U.S. 113 (1973).

[35] 478 US 186. Virtually all commentators argue that *Bowers* is at tension with *Roe*. Lawrence Tribe, who successfully litigated *Roe*, apparently lost *Bowers* partly through a strategic mistake: he did not make an equal protection argument, on the assumption that the court would be willing to extend privacy doctrine, hoping to get a second ruling that made the equal protection claim explicit. As it was, the court went out of its way to avoid looking at any pro-privacy argument which was not explicitly made.

not confined to sexuality. For example, Etzioni suggests the need for balancing privacy with other rights in general, and for doing so on a case by case basis. For example, he argues that more privacy is needed when dealing with medical records, but less in dealing with encryption, because "although many of the dangers are hypothetical (for instance, a terrorist holding a nuclear bomb, threatening a city), the disutility of any such dangers is so high that greater attention to public safety seems justified."[36] One should note in this context that for Etzioni, as for many thinkers, privacy needs to be thought of in terms of risk.

Privacy as a right or a protection has advantages and disadvantages, both of which are based on the very idea that certain spheres of relationships ought to be outside the public eye. The advantages should be evident from above, but one should note that many scholars (feminists in particular) argue that privacy is counterproductive in achieving women's freedom, precisely because it conceals objectionable activity from public scrutiny. For example, should the special privacy extended to marriages extend to providing protection for people in abusive relationships?[37] What about the protection of children from abusive parents? Those who applaud privacy decisions in general have been made uncomfortable by the Court's ruling in *Deshaney v. Winnebago*.[38] Joshua Deshaney was a four year old child beaten so severely by his father that he suffered brain damage which would confine him for the rest of his life to an institution for the severely retarded. Joshua's mother, acting as his agent, brought suit against Winnebago County, Wisconsin, the Department of Social Services (DSS) and other affiliates, charging that the DSS "deprived Joshua of his liberty without due process of law, in violation of his rights under the Fourteenth Amendment, by failing to intervene to protect him against a risk of violence at his father's hands of which they knew or should have known" (193). Citing its ruling in the decision against state-provided abortion funding, the Court ruled that the government had no positive obligation to provide for liberties which it could not take away: the private violence of Randy Deshaney against his son was outside the state's jurisdiction. The Court concluded:

> The most that can be said of the state functionaries in this case is that they stood by and did nothing when suspicious circumstances dictated a more active role for them. In defense of them it must also be said that had they moved too soon to take custody of the son away from the father, they would likely have been met with charges of improperly intruding into the parent-child relationship, charges based on the same Due Process Clause that forms the basis for the present charge of failure to provide adequate protection.[39]

The line that privacy draws, in other words, can both protect freedoms and conceal violences and injustice. Strong encryption can assist both business and terrorists. It is perhaps for this reason that the protection of privacy is both so important and so controversial: insofar as individuals necessarily live in a society, that society has to decide how to draw its boundaries.

---

[36] Etzioni, *Limits of Privacy*, 185.

[37] In this sense, privacy as a distinction in law might be seen to be analogous to professional ethics as a distinction in general ethics: the discomfort with privacy expressed by many commentators seems similar to the discomfort with professional ethics, insofar as both treat certain sub-groups within society as being governed by a different set of standards than those used outside it.

[38] *Deshaney v. Winnebago*, 498 U.S. 189 (1989).

[39] *Deshaney v. Winnebago*, 203.

Privacy – What is to be done?[40]

The Court's discussion of privacy is illuminating because it draws attention to the extent to which privacy involves contested social values. On the other hand, as a matter of constructing policy to protect privacy in the realm of computers, the Court's privacy decisions are less helpful. First, Supreme Court decisions either validate or invalidate state (or federal) laws on a constitutional basis. This means that if one's claim does not rise to a constitutional level (such, as the Court suggested, as was the case with Joshua Deshaney), the Court's rights decisions offer little protection. This also means that the Courts offer little protection to individuals from corporations, since those corporations are not the government.[41] Not only that, as noted above, the loss of privacy to corporations offers many material benefits.

The allure of benefits to loss of privacy leads to another difficulty in seeking redress in the Courts. First, when one gives up privacy to private parties, there is a structure of consent: one does not have to type in one's email address to a website; one could choose not to visit the site. Even in the extreme case of medical privacy, one does sign a consent form authorizing the release of the medical information. Whether or not this is consensual in practice becomes invisible to the legal point that once one has consensually disclosed information, one cannot then complain about its use.[42] An analogous situation applies in respect to speech: once I have said something – even something to which I own the copyright – I am not free to control the use made of it by members of the public. This principle runs very deep; one might even suggest that it is implicated in the public/private distinction itself, since the notion that one has released private information to the public suggests that it can no longer be treated as private. In short, there seems to be little constitutional basis for protecting individual privacy in most of the situations that apply online.[43]

One of the main ways that websites collect information about their customers is through the use of "cookies." Cookies are small files that the website deposits on the individual consumer's computer which collect information about that consumer. When next accessed, the site accesses the profile of the consumer. Cookies thus enable websites to tailor their presentation to the habits of consumers. Those who are alarmed at this practice do have one option, although it is hardly a panacea. One can disable cookies on one's browser. The importance of cookies is indicated by the fact that many websites will then complain that your browser has cookies disabled.[44]

As a more systemic level, several strategies have been suggested. The most popular seems to be "self-regulation," since

---

[40] Most of the following current examples are taken from Major R. Ken Pippin, "Consumer Privacy on the Internet: It's 'Surfer Beware,'" *Air Force Law Review* 47 (1999), 125-161.

[41] *Cf.* Deborah G. Johnson's *Computer Ethics*: "Our American forefathers were concerned about protecting us from the power of government …. They did not envision the enormous power that private organizations might have over the lives of individuals. Corporations are treated, in law, as persons in need of protection from government, rather than as powerful actors that need to be constrained in their dealings with individuals. We need to consider broad changes that would address this gap in our tradition" (98).

[42] "what a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection" (quoting *Katz*). This citation, as well as citations to other court cases and discussion, can be found at Pippin, n. 103.

[43] At least, not federally. Some state constitutions have privacy clauses. Etzioni suggests that the fourth amendment would adequately protect medical records.

[44] For a survey of website intrusions into privacy, and individual strategies for countering these, see Brett Glass, "Keeping your Private Information Private," *PC Magazine* (July 21, 2000 [reedited]), at URL: http://www.zdnet.com/pcmag/stories/reviews/0,6755,2572515,00.html.

that offers the hope of solving the problem without involving government regulation. Self-regulation was originally the solution advocated by the FTC, although, as noted above, the commission has since reversed its position based on the overwhelming evidence that self-regulation is achieving very little in the actual protection of consumer privacy. An example of self-regulation is found in the online Privacy Alliance (OPA), a coalition of about 80 net companies which developed a set of guidelines to which a site could cohere. One big one is for a site to post its privacy policy. Another initiative is for sites to be certified by an outside party for their privacy practices, for which they get to bear a seal. Examples of this include "truste," initiated by the EFF; as well as BBBOnline, and WebTrust. Pippin suggests some of the difficulties with this approach:

> The existence of industry-wide information protection programs and sector-specific efforts raises the issues of the existence of uniformity among the different programs, what standards each program will apply, and whether the consumer will be able to understand the differences between each program's standards. With so many different approaches to the problem of Internet privacy, self-regulation as not yet proven to be the best possible solution (133).

Though self-regulation has limitations, the imposition of anything stronger would require legislation. The FTC, for example, does not have the regulatory authority to require companies to adhere to fair information practices. At the moment, the FTC's position is strictly advisory and as an advocate for the adoption of the fair information practices.[45] Also, for various reasons (such as the opposition of industry), net privacy legislation has failed repeatedly when introduced to state legislatures.[46]

One important piece of legislation which did pass is known as the "Child Online Privacy Protection Act" (COPPA, 1998). Websites directed at children must obtain parental consent before collecting personal info. "COPPA has four primary goals: to enhance parental involvement in a child's on-line activities in order to protect the privacy of children in the on-line environment; to help protect the safety of children in on-line forums such as chat rooms, home pages, and pen-pal services in which children may make public postings of identifying information; to maintain the security of children's personal information collected on-line; and to limit the collection of personal information from children without parental consent."[47] COPPA is not popular with web businesses, because compliance with it entails considerable cost. Site owners must ensure that they do not collect personal information about children

---

[45] *Cf.* Pippin: "Despite the Commission's leadership role, its conclusions and especially its recommendations on addressing on-line privacy concerns have met with mixed reviews and dissent from consumer privacy organizations, Congress, and from within the Commission itself. The Commission currently endorses self-regulation as the best option available, citing both improved self-regulation efforts on the part of the private sector and the difficulties for the federal government in responding quickly to technological advancements, as well as the fear of hindering electronic commerce. Notwithstanding its overall recommendations, the Commission has endorsed legislative efforts specific to the area of on-line privacy for children, recognizing the heightened vulnerability of children exploring the Internet" (135).

[46] "Attorneys General Strive for Net Privacy, Crime Solutions," *Reuters* (March 24, 2000).

[47] Pippin, 136.

below the age of thirteen without parental consent, and traffic, predictably, drops off by as much as 20% when consent is added.[48]

This piecemeal approach to privacy protection, where legislation largely is specific and reactive to a narrowly defined problem, has its drawbacks, which might be seen as the disadvantages to *not* having substantial federal legislation. A comparison with computer crime, where there is sustained and coherent federal legislation (see the following chapter) seems to disclose that neither solution works perfectly. One of the primary costs of the piecemeal approach is consumer confusion. Most people do not understand the situation, and how (in particular) the combination of the piecemeal and self-regulatory approaches do not protect people except in very narrowly described situations. In a survey conducted by the Georgia Institute of Technology, for example, 74.3 percent of the Internet users polled thought that web sites were prohibited from reselling personal information collected on them to third parties.[49] Of course, as the FTC report makes clear, this practice is conducted by *most* sites, and is perfectly legal.

Privacy as an International Issue

It is important to remember that not all countries and societies deal with privacy issues in the same way. In particular, the European Union's treatment of privacy has been very different from that in the U.S., and the differences have caused considerable tensions. Under the terms of the EU's Privacy Directive, which was implemented in 1998, member states are required to implement comprehensive legislation to protect the privacy of their citizens. The protections required include the following:

> When collecting information from an individual, those processing data (known as the "controllers") must disclose their identities, the purposes for the processing, and other information. Data can only be processed for the announced purposes, contrary to the common U.S. practice of permitting a company to use personal data for unlimited purposes. Before data can be provided to third parties for direct marketing, the individual must be informed and have the right to opt out free of charge. Those processing personal data must guarantee that individuals have access to their own personal data and the opportunity to correct that data. Other rules apply, such as special restrictions on the processing of sensitive data, including information about racial or ethnic origin, political opinions, or the processing of data concerning health or sex life.[50]

The privacy directive also establishes rules for the export of data from the European Union, and it is these regulations which have caused tension with the U.S., since U.S.-based web firms often do business with European citizens. According to Article 25 of the privacy directive, data about EU citizens can only be transferred to companies outside of the EU if the countries governing those companies guarantee an "adequate" level of privacy protection. It is

[48] "Net privacy law costs a bundle," *CNN.com* (May 16, 2000).
[49] Pippin, 140-141.

[50] Peter P. Swire, "Of Elephants, Mice, and Privacy: International Choice of Law and the Internet," 8, at URL: http://papers.ssrn.com/paper.taf?ABSTRACT_ID=121277. Swire discusses at length the difficulties which will face regulation of international commerce on the net, in particular which legal system will govern international commercial transactions and how legislators can respond to issues which they deem important.

the considered opinion of the EU that the U.S. does not even come close to this standard.

Since passing the privacy legislation, the U.S. and EU have agreed, at least in principle, to the passage of "safe harbor" legislation. According to the terms of this agreement, the U.S. government would maintain a list of companies with privacy policies which meet EU standards, and those companies would be allowed to transfer data about European citizens. Other companies would have to negotiate individually with the EU.[51] The EU is presently considering legislation which would ban spam (unsolicited commercial) email except for those who specifically "opt-in" to receiving it, and is threatening to take action to restrict the collection of cookies.[52]

The point to remember is that one of the issues highlighted by the ease with which data can be transferred around the world on the Net is that different governments have different views as to how this data should be managed. U.S. views on data privacy will necessarily be confronted with those of others. The necessity of confronting, and negotiating agreements about these differing values will be one of the more prominent issues highlighted by the global diffusion of information technologies.

---

[51] "Brussels ends data protection dispute with US," *Financial Times (London)* (July 28, 2000), 12. Passage of this agreement was not uncontroversial in Europe; many feared that the safe harbors did not provide enough privacy protection. See "U.S.-EU Net Privacy Proposal in Jeopardy," *The Standard* (June 26, 2000), at URL: http://www.thestandard.com/article/display/1,1151,16387,00.html.

[52] "EU to Restrict Use of Spam and Cookies," *The Standard* (July 26, 2000), at URL: http://www.thestandard.com/article/display/1,1151,16982,00.html.

CHAPTER V: COMPUTERS AND CRIME - DARK SIDES OF THE INTERNET

The rapid development of information technology and the "information economy" has brought with it the rapid development of "computer crime." Evidence of this is easy enough to find, from reports of virus or denial of service (DoS) attacks to the frequent requests by the Department of Justice for more resources to handle computer crime. The topic of computer crime is difficulty partly because it is difficult to define exactly what constitutes a computer crime, particularly since legislation often lags behind the ability of people to do undesirable things on a computer. For example, the Philippine government was initially unable to successfully prosecute the student who apparently released the "love bug" virus because the country's anti-hacking legislation had not yet been signed into law.[1] For the purposes of this chapter, then, I wish to consider computer crime in the broad sense of socially undesirable behavior which is either unique to, or made substantially different and worse by, the diffusion of information technology. Before discussing the federal legislative response to computer crime, then, I wish to begin with two very different examples of such behavior. The differences between will underscore both the real human cost of computer crime, and the extent to which "traditional" criminal activities are adaptable to the Internet.

Denial of Service Attacks

The Spring, 2000 denial of service attacks are exemplary of a new form of crime which is both unique to computer systems and which had not been attempted on a wide scale before. They thus illustrate the amenability of the "information infrastructure" to unexpected attack. For a period of a few days beginning February 7, 2000, a number of major Internet sites were flooded with phony connection requests. Bogged down by efforts to handle these phony requests, the entire site slowed to a crawl or even crashed. Targeted sites included amazon.com, E*Trade, ZDNet, and (somewhat later) CNN.com.[2] The situation might be analogized to rush hour traffic, except that most of the cars on the road are empty: access for drivers is impeded, not by other legitimate drivers, but by the empty vehicles. Within a few days, the FBI had narrowed a suspect list to include an American and a Canadian, using a program apparently written in Germany.[3] There were already a series of difficult ethical questions posed: the German who wrote the program denied responsibility for the attacks, suggesting that they provided a public service to the Net community by pointing out its security flaws.[4] One prominent computer professional has compared this to setting fire to a shopping mall in order to demonstrate that it needs a sprinkler system: the damage is still done.[5] Still, questions of responsibility remain; one might still ask, to what extent is the damage done by a dangerous program the responsibility of its creator? As we will see, the American computer crime law is assigning increasing responsibility for such "unintentional" damages.

As the story developed, it became more complicated. First, the computers which initiated the attack were themselves victims: at least one computer at Stanford University and another at the

[1] "Love Bug Suspect Freed," *CNNfn.com* (June 7, 2000). The Philipines later pressed charges under a credit card fraud law.

[2] "E*Trade, ZDNet latest targets in wave of cyber-attacks," *CNN.com* (February 9, 2000)

[3] "Leads Narrow List of Suspects in Web Attacks," *Wall Street Journal,* 02/14/00, P. A3.

[4] "Hacker Proud of Program, Denounces Web Attack Use," *Los Angeles Times* (February 12, 2000), A1.

[5] Eugene Spafford, "Are Computer Hacker Break-ins Ethical?" in *Internet Besieged,* eds. Dorothy E. Denning and Peter J. Denning (New York: ACM, 1998). 493-506.

University of California, Santa Barbara (UCSB) had "zombie" programs installed on them. These zombie programs were then activated remotely, and used the university computers as a platform from which to launch the phony service requests. This, in turn, suggested a further and substantial problem, since any computer which is online the whole time is a potential target. In other words, virtually any computer with a broadband connection to the net could have been used. This means, as one article put it, that "many, if not most, of the computers that were actually hacked remain compromised;"[6] a computer networking person at UCSB pointed out that the computer used was "wholly unremarkable."[7] Further questions emerged: to what extent are computer users responsible for attacks carried out from their machines? These questions became particularly acute when the news media discovered that the Computer Emergency Response Team (CERT), a national group based at Carnegie Mellon University which provides resources for dealing with computer crime and infrastructural issues, had issued a warning in December, 1999, about the probability of exactly such an impending denial of service attack. Some pointed fingers at companies which did not take adequate (or any) security measures; one industry spokesperson offered in response that "you didn't have widespread attention to the fact that the warning was out there, and you didn't have widespread action that would have prevented attacks from occurring …. It was noise in the background." Others pointed out the high vulnerability of university computers, but wondered aloud the extent to which universities should be expected to pay the bills for an insecurity brought on primarily by the commercialization of the Internet.[8]

One immediate effect of the attacks was economic. Not only did the sites attacked lose revenue, but numerous commentators warned of the possibility of a loss of confidence in the net economy in general. One should recall both the tremendous amount of money involved in this economy, and its relative fragility, as evidenced by the instability of technology stocks. As one security expert put it, "These organizations that have been attacked this week have suffered revenue loss … [and] their own customers' confidence in them has been shaken. It will have a ripple effect in the whole industry as far as confidence in e-commerce and e-commerce viability."[9] Actual loss estimates varied widely, but all were sobering. One research group estimated losses at $1.2 billion.[10] A survey conducted shortly after the attacks reported that those surveyed were 45% less likely to transmit credit card information online as a result of the attacks (even though the attacks had nothing to do with the loss of credit card information), and the technology-stock driven NASDAQ dropped 65 points the day after the Yahoo! Attacks. As one editorial put it, "much concern has been churned up about the dangerous possibility of hackers getting into the computers of the defense sector. But attacks which have

---

[6] IDG News Service (Feb. 11, 2000), at URL http://www.idg.net/idgns/2000/02/11/RealDoSHackVictimsWerentWeb.shtml

[7] "University of California Computer used in Attacks," *Network World Fusion* (Feb. 14, 2000), at URL: http://www.nwfusion.com/news/2000/0214computerfound.html .

[8] For the CERT warning, see "CERT Warns of Networked denial of Service Attacks," *Computerworld* (December 23, 1999), and "High Tech Industry Plans to Unite Against Hackers," *Los Angeles Times* (February 16, 2000), A13. For the discussion of university vulnerability, see "Inside Track: Weak Links Put the Web at Risk," *Financial Times (London)* (February 16, 2000).

[9] Qt. in *ibid*.

[10] This story is reported by the Chinese Xinhua service: "Web Hacks Cause 1.2 Billion Dollars in Losses," *Xinhua General News Service* (February 15, 2000). The "Yankee Group" press announcement is at URL: http://www.yankeegroup.com/webfolder/yg21a.nsf/press/384D3C49772576EF85256881007DC0EE?OpenDocument.

economic implications could bring about equally horrifying results. Imagine the chaos if the world's payments system were attacked, or if computers managing currency exchange markets suddenly crashed, or if those manning the global navigation system suffered a similar intrusion by hackers."[11]

The warnings about economic attacks reached almost apocalyptic tones. Dr. Aharon Friedman, a network security consultant to the Department of Defense, opined that "intrusive attacks on unprotected sites will have alarming and lasting consequences to both the US economy and the US psyche. You can be certain that many hostile groups have taken note of how vulnerable US commerce is to cyber attack."[12] A conference sponsored by the prestigious Brookings Institute warned that despite such attacks, the U.S. electronic infrastructure remained dangerously insecure, and that one of the primary problems was a false sense of security generated by the absence of a truly devastating attack.[13] At issue, then, are fundamental questions about what it means to be a "secure" society and the level of risk one is willing to accept.

Various solutions have been suggested, some of them technological. For example, researchers at one security firm proposed "cryptographic" puzzles. A computer which wishes to establish a connection with another online sends a "SYN." The computer which sends the SYN then responds with a SYN-ACK, and leaves an open connection, waiting for a final ACK as confirmation. The denial of service attacks, then, worked by sending millions of SYN signals, forcing targeted computers to spend all of their resources opening, and keeping open, false connections. According to the cryptographic puzzles proposal, a computer desiring a connection could initiate that connection with an "are you being attacked" message. If the answer is yes, the computer responds with a short puzzle for the initiating computer to solve. The responding computer then does not allocate further resources until the puzzle is returned correctly solved. In this way, attacking computers are themselves slowed down.[14] From the point of view of solving the problem, the technological solution remains that: even if one concedes that it would work, it remains limited to this specific denial of service attack, and, more importantly, would likely require years of research and advocacy before enough systems adopted it as a standard to have a noticeable effect on the net as a whole. Others suggested a direct counterattack. Attacked computers could launch a denial of service or other disabling assault on those computers attacking them. This approach, however, raises numerous ethical questions, particularly in this case because the attacking computers were generally zombies and themselves "innocent."[15]

Denial of Service and other computer attacks also lead to calls for legislative action. Following the February, 2000 attacks, President Clinton held a security summit with industry leaders on February 15; the Congressional Joint Committee on Commerce met on Feb. 23, and the Senate Judiciary Committee, chaired by Orin Hatch (one of the primary architects of the DMCA) announced

[11] The survey is cited in "High Tech Industry Plans to Unite Against Hackers;" for the economic NASDAQ data and editorial warning, see "Putting a firm stop to computer hackers," *Business Times (Malaysia)* (February 16, 2000).

[12] "Worst Hacker Attacks Yet to Come," *PR Newswire* (February 15, 2000).

[13] "False sense of cybersecurity a costly problem for U.S.," *CNN.com* (June 20, 2000).

[14] Ari Juels and John Brainard, "Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks," at URL: http://www.rsasecurity.com/rsalabs/staff/ajuels/papers/clientpuzzles.pdf.

[15] For discussion, see Deborah Radcliff, "Hack Back," *Network World* (May 29, 2000).

hearings for March.[16] Attorney General Janet Reno and FBI director Louis Freeh appeared before another Congressional Committee to request an almost 40% increase in the resources devoted to fighting computer crimes in general.[17]

Mail Order Brides and Prostitution

Not all computer crime is limited to the Internet, and not all of the victims of computer crime are necessarily themselves computer users. As the popularity of sites such as amazon.com, E-Bay, and others indicate, the Internet is a wonderful place to buy and sell things. From the point of view of sellers, one advantage of net sales is the comparative lack of regulation. Not only are net transactions often tax-free, but often activities which would be shut down by local authorities in "bricks and mortar" businesses can thrive online, as the difficulties states experience in enforcing their gambling laws online attest. A particularly dark form of this commerce is in people, specifically women from developing countries. By this I do not mean pornography, but the direct purchase and sale of human beings. According to a CIA report completed in December, 1999, over 50,000 women *per year* are duped into the United States through advertisements, for example, for phony *au pair* services, and then forced or sold directly into prostitution.[18] Another such inducement is the mail order bride business.[19]

It is easy to compile data as to the scope of the problem: Typing the phrase "mail order bride" into AltaVista, a popular search engine, generated 10,115 results. Of the first ten, most were sites offering women as products.[20] For example, "rdreamdate.com" advertises "Russian dream dates," and generates frequent pop-up ads to other "dating services." It presents an "order form," for which the user enters information about such characteristics as minimum and maximum desired age, height, and weight. The site then generates a list of thumbnail photos; clicking on those leads to a page for each woman. This page includes full-body photos, of which one is bikini, and a brief biography of the woman, listing her city of residence, age, level of English proficiency, and the sorts of things one might find in a personal ad. For example, many women report being in search of a man who "enjoys being a husband."[21] Another of the first ten sites on AltaVista featured a flashing banner of "2700 women available." In all cases, users pay for increased levels of access to the women, up to and including a trip to, for example, the Philippines, on which one is afforded the opportunity to view an "unlimited" number of women before selecting one. After selection, the agency provides assistance with her immigration paperwork.

---

[16] "White House, Congress to Hold Separate Meetings on Hacker Attacks," *Computer World* (February 11, 2000), at URL: http://www.computerworld.com/home/print.nsf/idgnet/000211E9B6.

[17] "Clinton administration develops Internet security proposals as investigators pursue hackers," *CNN.com* (February 16, 2000).

[18] "Thousands brought to U.S. annually as prostitutes report says," *CNN.com* (April 2, 2000).

[19] For a sustained description and critique, see Donna R. Lee, "Mail Fantasy: Global Sexual Exploitation in the Mail-Order Bride Industry and Proposed Legal Solutions," *Asian Law Journal* 5 (May 1998), 139-179.

[20] http://www.altavista.com, visited April 2, 2000.

[21] *Cf.* Lee, "Mail Fantasy:" "While agencies frequently provide the women's hobbies below their photographs, this may well be a tactic to alert the men to women likely to make traditional wives, rather than to ensure that the women, by describing their interests, will find someone compatible. There is surprisingly little variation in the hobbies listed, cooking being one of the most common. No doubt women list hobbies that they believe are desired by men in industrialized nations. In any case, agencies generally present the women in such a way that men are encouraged to choose the women with whom they want to correspond primarily on the basis of appearance; the women's interests become a secondary consideration" (144-145).

These advertisements (and the business in general) reinforce cultural stereotypes at every step. For example, they present Asian women as racially submissive, as well as playing on cultural stereotypes about "Asian beauty" or "Oriental charm." Virtually all of the targeted women come from countries where economic conditions are severely bad and/or social expectations are for immediate marriage. Many are desperate for a way out of their social situation, and all are fed advertising regarding the chivalrous and providing characteristics of American men. Hence, Russia and the Philippines are main sources, among other places.[22] As for the American man who purchases them, "the typical customer is an older Caucasian man, who joins a mail-order bride agency in search of an 'eternal treasure' or that 'special lady.' He is often divorced and disenchanted with the feminist movement, attributing his failure at relationships or marriage to what he considers to be the intolerable attitude of feminist women."[23]

This activity flourishes on the Internet as never before. There are several reasons. First, sites are relatively anonymous and difficult to trace. Particularly for merchants in countries with weak or bribable law enforcement, it is easy to operate whether or not the activity is legal. For customers, shopping through the Internet provides the same advantages it does when one is shopping for anything else: there is a greater range of available "products," and the shopping can be done in the privacy of one's own home, without the need for embarrassing trips to dodgy stores or the receipt of embarrassing literature in the mail. As a practice, then, the process is virtually impossible to track, and in most countries it is not illegal. Indeed, it would be hard to understand how to make it illegal without essentially prohibiting all international marriages. The history of international marriage law in the United States is testimony to these difficulties. The Marriage Fraud Act had (essentially) made it a deportable offense for an immigrant to marry an American but to stay married for less than two years. Under pressure from women's' rights groups, who pointed to widespread abuse of women who were threatened by their husbands with deportation, this legislation was repealed as part of the 1994 omnibus crime bill. However, there is still a two year requirement built into the code of federal regulations. Although one can be exempted from this requirement, obtaining the exemption requires not only knowing that it exists, but often obtaining the testimony of an independent social worker. Furthermore, the INS still does not grant work authorization to women who petition for the exemption, forcing them into a decision between an abusive husband and no job. These requirements can be unobtainable for those who most need them.[24]

The combination of predatory, overtly misogynistic men, clever advertising, vulnerable and economically desperate women creates a lucrative trade in fraudulent marriages, undertaken for motives unrelated to love. The combination of these fraudulent marriages and regulatory efforts to combat them while still allowing legitimate marriages is often catastrophic for the individual women involved. Many women are brought to the U.S. on "finance" visas (K-1), which are granted on the expectation of impending marriage. Dumped almost immediately by their sponsors and lacking a work permit to work legally, they can be forced into prostitution simply to raise the cash to buy a plane ticket home. For those who are

[22] Russian and Eastern European liason sites showed up on my AltaVista search of 4/2/00; see Lee, "Mail Fantasy" for the predominance of Philipine sites among Asian sites and the social structures which drive Philipino women to such "services."

[23] Lee, "Mail Fantasy," 145.

[24] For a history and critical discussion of these requirements, including the frequent disparity between Congressional intent and INS implementation, see James A. Jones, "The Immigration Marriage Fraud Amendments: Sham Marriages or Sham Legislation?" *Florida State University Law Review* 24 (Spring 1997), 679-701.

actually married to their sponsors, the situation can be equally as bad, if not worse:

> Lacking the necessary language skills, women often sign papers indebting themselves to those who bring them into the country. Even in the absence of such a signed agreement, a mail-order bride may find that the substantial expenses incurred by her husband in acquiring her are later used as a tool to reinforce control over her. These expenditures tend to give men a sense that they are entitled to recoup their costs through sexual services, housekeeping, or other labor. Some brides are reduced to no more than 'better-class slaves...I've also seen cases where husbands forced their wives into prostitution privately with their friends.' In fact, Philippine embassies in Europe have reported that a number of match-making agencies are simply fronts for prostitution rings preying on newly-arrived Filipinas."[25]

The point, then, is that "computer crime" is not limited to sterile-sounding cases of hackers and e-commerce sites. The very pervasiveness of information technology is leading to the pervasiveness of socially undesirable activity accompanying it. Many times this activity is not addressed by legislation, and it is often difficult to understand how it could be addressed. Other times, it is illegal but difficult to enforce.

[25] Lee, "Mail Fantasy," 152, citations omitted.

Analysis and Discussion

Examples of computer crime could me multiplied indefinitely. Some of these issues have already been discussed: cyberstalking and identity theft, for example. Others include computer versions of credit card fraud and blackmail. One Russian hacker, for example, stole credit card numbers from web merchants and then posted them on the Internet when the company refused to pay a $100,000 ransom for their return.[26] A disgruntled New Jersey employee was convicted of writing a software bomb, which crippled his former employer's system and caused an estimated $12 million in damages.[27] Internet worms, which spread through emailed file attachments, are rampant. Most, such as the "Love Bug" and "Melissa," operate by sending themselves to everyone in a Microsoft Outlook address file, and then doing some sort of damage to the computer. Indeed, protection from such malicious code has become an important sub-industry in its own right, and an essential for computer users.[28] Opening unsolicited email attachments recently topped a Department of Justice and FBI list of "most dangerous" threats to computer security. The list also included failing to employ adequately trained security personnel, installing systems without adequate firewall and other protections, and so forth.[29] As indicated above, efforts to combat computer crime are frequently the subject of national attention, and there was recently a

[26] "Rebuffed Internet Extortionist Posts Credit Card Data," *CNN.com* (January 10, 2000).
[27] "Legal system gears up for computer crime cases," *CNN.com* (June 27, 2000).
[28] For updated virus listings, see the sites of virus protection companies, e.g., datafellows.com (F-Secure products). Virus protection is so lucrative the F-Secure Corporation (which trades on the Helsinki exchange) split 5:1 in Spring, 2000.
[29] "FBI, DOJ Issue List of Worst Net Threats," *The Industry Standard* (May 31, 2000), at URL: http://www.thestandard.com/article/display/1,1151,15608,00.html.

conference in Paris designed to improve international cooperation on the issue.[30]

The following discussion revolves around U.S. federal law. It does not cover state laws, or international issues (some of which will be discussed in the following chapter), even though many of the issues at hand are international in scope.[31] The examples given above are illuminating because most people can agree that they describe a "bad thing." However, at the same time, it is difficult to imagine any solutions which would both solve the problem and operate without trampling on the rights of law-abiding citizens. In particular, free speech rights often conflict with computer law enforcement. Some aspects of this conflict have already been discussed with regards to intellectual property and privacy, but it extends, as the discussion below indicates, to cover such areas as pornography. As an initial analytical point, then, it is important to note that "computer crime" is a *broad* term – it includes both computer versions of old crimes, and "novel, technologically specific offenses that are arguably not analogous to any noncomputer crimes."[32] The Department of Justice defines "computer crime" as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution."[33] Partly because the issue is so broad, and encompasses not just violations of existing law but also discussions of what new laws should be passed, issues in computer crime often implicate deeply held social values over which there is little consensus. Various polar positions tend to emerge in legislative and enforcement debates: some advocate free speech over all other concerns; others argue that law enforcement or "security" should trump other concerns. Business also has a substantial stake, and faces a similar conceptual difficulty. On the one hand, businesses want strong protection against crime. On the other hand, such strong protection implies intrusive legislation which might interfere with the corporate goal of a free market. One issue seems obvious: crime is a human problem, and if information technology offers an occasion for new forms of criminality, the technology itself is neither the cause nor the solution.

Much of the debate centers around notions of responsibility, and the extent to which an individual can be held responsible for actions which he or she might not have directly precipitated. In this regard, a pair of distinctions should be highlighted. First, law makes a distinction between an intentional and an unintentional act, usually punishing more severely an act which is intentional. For example, in a distinction which will be familiar and which most states make, Tennessee law divides "murder" into three categories. "Murder" *per se* refers to the pre-meditated, intentional taking of another human life. "Manslaughter" implies intentional killing, but not necessarily planned in advance. "Negligent homicide" describes an act which unintentionally causes the death of another person but which the actor should have foreseen. An example of negligent homicide is dropping rocks off a bridge onto the interstate: one may not plan to kill anyone, but one should know that the activity is likely to do so. All three kinds of killing are punishable, but the severity drops the less the act is considered intentional. In the case of computer ethics and crime, the question of intent is closely related to a question of professional ethics in general, that of the degree to which those who know about the technology are more responsible than those who do not. For example, if I know nothing about computers and open a file attachment containing a virus that destroys my company's computer system, I might be less culpable than if as a programmer I do the same thing. Second, and as a

---

[30] "World's Leaders Unite to Battle Cybercrime," *Toronto Star* (May 15, 2000).

[31] For some of these concerns, see also the closing pages of Michael Hatcher, Jay McDannell and Stacy Ostfeld, "Computer Crimes," *American Criminal Law Review* 36 (Summer 1999), 397-444.

[32] Hatcher, McDannell and Ostfeld, "Computer Crimes," 398.

[33] *Qt*. in Hatcher, McDannell and Ostfeld, "Computer Crimes," 399.

corollary, acts committed for fun (without criminal intent) are not thereby excused, even if no damage occurred. In this sense, the law is not always utilitarian, and the 1996 computer crime legislation explicitly codifies this idea.

Federal Computer Crime Legislation

Unlike its adoption of piecemeal privacy legislation, Congress has attempted to deal with computer crimes as a class, and under one piece of legislation. The Department of Justice classifies computer crimes into three groups:

> 1. A computer may be the 'object' of a crime: the offender targets the computer itself. This encompasses theft of computer processor time and computerized services.
>
> 2. A computer may be the 'subject' of a crime: a computer is the physical site of the crime, or the source of, or reason for, unique forms of asset loss. This includes the use of 'viruses,' 'Trojan horses,' 'logic bombs,' and 'sniffers.'
>
> 3. A computer may be an 'instrument' used to commit traditional crimes in a more complex manner. For example, a computer might be used to collect credit card information to make fraudulent purchases.[34]

[34] Hatcher, McDannell and Ostfield, "Comp uter Crimes," 401, citations omitted and numbering breaks added.

The first major federal attempt to deal with computer crimes was the Computer Fraud and Abuse Act (CFAA) of 1986. Subsequent legislation includes amendments to the CFAA in 1988, 89, 90, and 1994 and the National Information Infrastructure Protection Act (1996). The NIIPA will be the locus of the following discussion. It should however be noted that computer crimes can also be prosecuted under Copyright Act, the National Stolen Property Act,[35] mail and wire fraud statutes, the Electronic Communications Privacy Act,[36] the Telecommunications Act of 1996,[37] and the Child Pornography Prevention Act of 1996.[38]

Despite all of these laws, there are relatively few prosecutions (except for child pornography). There seems to be a bit of a chicken and egg problem. One reason seems to be low reporting: apparently only 17% of those organizations which suffered losses from computer crime reported them. Apparently they do not want to look

[35] The NSPA "prohibits the transportation in interstate commerce of 'any goods, wares, securities or money' valued at $ 5,000 or more and known to be stolen or fraudulently obtained. This statute has been applied to various computer-related crimes, including fraudulent computerized transfers of funds" (Hatcher, *et. al*., 412-413).

[36] This 1986 law basically tries to stop the interception of electronic communication.

[37] See the discussion below, on the Communications Decency Act (CDA), which was a part of this law.

[38] According to Charles Platt, *Anarchy Online* (New York: Harper Prism, 1996), this was part of the same scare that generated the CDA. Hatcher comments on the CPPA, which was passed "to prevent the production and distribution of computer-generated, sexual images of children. The CPPA criminalizes the production, distribution, and reception of images that are electronically or mechanically created or altered to render sexual depictions of minors. Thus, the CPPA prohibits computer transmission of erotic photographs of adults doctored to resemble children. The constitutionality of the CPPA is an open question and currently in dispute in the district courts" (Hatcher, *et. al*., 418, citations omitted).

weak or vulnerable.[39] Industry spokespeople, however, point to the low success rate of the Department of Justice. According to internal DoJ statistics, only one cybercrime is prosecuted for every fifty complaints, which is not a success ratio that companies feel is worth the risk of governmental scrutiny and possible subsequent loss of proprietary information.[40] What had been a request for $37 million after the denial of service attacks became a request for over $75 million in new funds on the part of the FBI by April, including substantial new resources for surveillance and data-collection.[41]

The National Information Infrastructure Act (NIIPA) of 1996 makes a number of innovations over previous versions of the CFAA.[42] First, it expands coverage to any computer(s) connected to the Internet, no matter what state they're in. Previously, the computers had to be in multiple states to be within federal jurisdiction, precluding prosecution of crimes committed where both computers were within the same state. Second, the NIIPA makes it a crime to access computer files without authorization or in excess of authorization, and subsequently to transmit classified government information. Third, it prohibits obtaining, without access or in excess of authorized access, information from financial institutions, the U.S. government, or private sector computers used in interstate commerce. Fourth, it prohibits intentionally accessing a U.S. department or agency nonpublic computer without authorization. It removes the word "adversely" from the statute, which means that you can no longer defend yourself by saying "I didn't do any harm." Finally, the act prohibits accessing a protected computer, without or beyond authorization, with the intent to defraud and obtain something of value.[43]

The NIIPA also cleared up various statutory confusions and increased the list of things which would fall into the category of unauthorized hacking. In particular, the 1994 act was unclear about whether hacker attacks had to be from out of state. As of the 1996 act, they are all criminalized, regardless of where they come from. The original CFAA also required, in order to prosecute, that damage be done by those without authorized access. Hence, an insider could damage a system and be exempt from the federal computer crime law. The update also covers insiders and others with authorized access. Those without access are liable for *all* damage they cause, whether intentional or not; those with access are only liable for intentional damage.

Increasingly, in other words, the law is coming to reflect a broad social consensus that "hacker ethics" simply are not ethical. Deborah G. Johnson, in her textbook discussion of computer ethics, summarizes four typical defenses of unauthorized hacking: (1) information should be free; (2) break-ins illustrate security problems and thus do a service for the computing community; (3) hackers are learning about computers rather than doing damage; and (4) hackers watch for abuse to keep big brother at bay.[44] If these arguments ever did make sense, they make increasingly less such sense as computer technology becomes more widespread. The first argument, for example, might or might not be correct, but it is incompatible with the functioning of a free market. While there is no doubt that some information should be free, this does not imply that all information should be free any more than the idea that some information should be owned implies that it all should. In other

[39] See Hatcher, *et. al*., 433.
[40] "Valley Cool to Cybercrime Plan," *Associated Press* (April 6, 2000).
[41] "'Digital Storm' Brews at FBI," *Washington Post* (April 6, 2000), p. A1.
[42] The following is drawn, almost verbatim, from Hatcher, *et. al*., 403ff.
[43] There is an exception if the defendant only obtained computer time with a value less than $ 5,000 per year.
[44] Deborah G. Johnson, *Computer Ethics*, 112-118. See also Eugene H. Spafford, "Are Computer Hacker Break-ins Ethical?"

words, it contradicts another premise that hackers often hold dear. The second is refuted by the example of the authorship of the code launching denial of service attacks; this experience also strongly presses the third justification. The third justification also begs the question of whether unauthorized hacking is a good way to learn about computers, and whether the information learned is not less valuable than the damage caused. The final example not only presupposes a vigilantism which most people would find suspect when applied to instances of weapons hoarding and paramilitary exercises, but also undoes itself: calls for big government crime legislation *almost always* follow hacking attacks. These points have been debated many times before; I wish to highlight here the extent to which the federal computer laws have increasingly not just criminalized unauthorized access, but also closed loopholes based on these four types of justification.

Before closing discussion of the NIIPA, a few more provisions should be noted. First, the act prohibits knowingly trafficking in passwords or something that would allow unauthorized access. Second, a new section added in 1996 makes it illegal to transmit in interstate or foreign commerce any threat to cause damage to a protected computer with intent to extort something of value. This section would cover such offenses as hackers threatening to crash a system if not given system privileges, or encrypting someone's data and demanding money for the key. Most of the offenses listed in the act are felonies if committed for financial gain, in furtherance of another criminal act, etc. Victims can also sue for civil remedies. Finally, in some cases, attempts at computer crime can be punished whether or not they succeed.

Pornography

Few computer-related topics, it seems, generate as much legislative attention as the ready availability of pornography online.[45] In particular, legislators are concerned to protect children from stumbling onto pornographic sites accidentally (or deliberately). Computer pornography is exemplary of the complex ethical, political, and social issues surrounding the diffusion of computer technology. In this case, the questions are much the same as in other debates about pornography, except that the stakes are suddenly much higher because pornographic material is suddenly much more available, being accessible to anyone with a net connection and a browser. Suppose that pornography is defined as the graphic depiction of sexual activity. A host of issues immediately arise. How important is free speech, even if it offends (and who sets the standards for "offensive")? Is pornography even really speech at all? Is porn prostitution? Should that be allowed? Does the mere existence of a society which tolerates pornography demean the status of women? What about lesbian and gay porn? Does watching pornography increase the chances that men will commit crimes? Should those who live in a less tolerant community thereby have less access to porn? What makes something "obscene," and what is a "redeeming literary or social value" to weigh against obscenity? Is all graphic display of sexuality pornographic? Where does one draw the line between pornography and art? These questions have inspired virulent debates, and pornography is for many people a test case for fundamental values, whether those are free speech or the social objectification of women.

---

[45] The relative amount of attention may be only apparent. One commentator has suggested that the flurry of attention surrounding online pornography has obscured the very real, and lengthy list of legislative advances made by the copyright industries in making it increasingly difficult to post non-commercial ("free") speech online. See Jessica Litman, "Electronic Commerce and Free Speech," at URL: http://papers.ssrn.com/paper.taf?ABSTRACT_ID=218275

In what follows, I will not enter this debate. Rather, I wish to track the fate of Congressional efforts to regulate Internet pornography, because they are exemplary of the challenges faced by efforts to deal with computer crime, and to set social standards for what sort of behavior should and should not be criminal. One fact forcing the debate is market-oriented: net pornography is big business. As of 1998, pornography was the third largest area of sales on the Internet with an estimated annual revenue of $100 million. Many adult Internet sites are accessed more than two million times in a one-month period. The scope of the issue generates concern: 85% of Americans indicated their concern with the issue.[46] On top of whatever one thinks of decency, Internet regulation of pornography faces at least two additional difficulties:

> There are two characteristics which make regulating the Internet very difficult, its decentralization and openness. Simply stated, 'no one owns the Internet, thus no one controls it.' It is open to anyone with a computer and modem, unbounded by geographical barriers, and its content 'is as diverse as human thought.' Therefore, controlling the content of the Internet is extremely difficult because no one knows where the material originates, who is receiving the material, or if it has crossed international boundaries.[47]

These difficulties have not prevented Congress from trying. The first such Congressional effort was the 1996 Communications Decency Act (CDA), which was inserted into a larger telecommunications reform bill. Substantial portions of this act were struck down as unconstitutional restrictions on free speech by the Supreme Court in *Reno v. ACLU*.[48]

The CDA has an odd history, a history which discloses the depths of feeling that pornography can invoke. In 1995, Marty Rimm, listed as a "Researcher and Principal Investigator, College of Engineering, Carnegie Mellon University" and citing support from four grants, published in the *Georgetown University Law Journal* an article which purported have "undertaken the first systematic study of pornography on the Information Superhighway."[49] After lengthy (and very graphic) descriptions of his categorization schema, through which an image and its description were categorized either as pornographic or not, and then by type of pornography, Rimm reached a number of startling conclusions. For example, "83.5% of all images posted on the Usenet are pornographic. This suggests that the next wave of multimedia products, designed to make the Usenet more 'interactive,' may be fueled largely by pornography."[50] He concludes that paraphilia (S&M, Bestiality, etc.) and pedophilia

[46] Kelly M. Doherty, "www.obscenity.com: An Analysis of Obscenity and Indecency Regulation on the Internet," *Akron Law Review* 32 (1999), 266 n. 48. Doherty cites Brian M. Werst, "A Survey of the First Amendment 'Indecency' Legal Doctrine and Its Inapplicability to Internet Regulation: A Guide for Protecting Children from Internet Indecency After *Reno v. ACLU*," *Gonzaga Law Review* 33 (1998), 209.

[47] Doherty, "obsenity.com," 265-266.

[48] *Reno v. ACLU,* 521 U.S. 844 (1997).

[49] Marty Rimm, "Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in over 2,000 Cities in Forty Countries, Provinces, and Territories," *Georgetown University Law Journal* 83 (1995), 1853.

[50] Rimm, "Marketing Pornography," 1914.

dominate online pornography: "the 'adult' BBS market is driven largely by the demand for paraphilic and pedo/hebephilic imagery. The availability of, and demand for, vaginal sex imagery is relatively small."[51] Indeed, he added with suspicious precision, that in his survey, "Pedo/hebephilic and paraphilic imagery accounts for 2,685,777 downloads, or 48.4%, of all downloads from commercial 'adult' BBS."[52]

Rimm's study became somewhat of a media sensation. It generated a cover article on *Time* magazine. Catherine Mackinnon, a prominent anti-pornography activist, celebrated Rimm's virtue in "documenting, with unprecedented scientific precision and definitiveness, who is using whom, where, when, and how."[53] The study suggested that everyone was using women online, that the expansion of access to the net would largely fuel expansion in access to pornography, and that net users preferred pornography which was not only pornographic, but illegal. Senator Exon promptly introduced the CDA, announcing that "the information superhighway should not become a red light district," adding later that "in my 8 years as Governor of Nebraska and my 17 years of having the great opportunity to serve my State in the Senate, there is nothing that I feel more strongly about than this piece of legislation."[54] A specter was haunting the Internet. Or was it? It turns out that Rimm's study proved almost nothing. As one commentator summarized:

> The problems of the Rimm Study were numerous. The Rimm Study was apparently not subject to peer review. Professors Donna L. Hoffman and Thomas P. Novak criticized the study, concluding that Rimm's work was methodologically flawed. The ethics of Mr. Rimm's research procedures were questioned. He was accused of plagiarism. Finally, it was discovered that he was working both sides of this issue; Mr. Rimm was also the author of *The Pornographer's Handbook: How to Exploit Women, Dupe Men, & Make Lots of Money*. In the end, even Carnegie Mellon, his graduate school, distanced itself from the Rimm Study. As a final salvo in the Rimm Study skirmish, the United States Senate decided that it no longer needed to hear what Mr. Rimm had to say about pornography and pulled him from the witness list of the July 26, 1995, hearing concerning pornography on the Internet.[55]

Even *Time* published a follow-up article, more or less apologizing for having been duped into publishing the story. Still, amidst great fanfare and in the middle of an omnibus piece of telecommunications legislation, Congress passed the CDA: legislation is often necessary in absence of "scientific" evidence of a problem.

That Rimm's study was largely invalid does not negate that pornography is easily available online. It also does not negate that this pornography is available to children, and that it can depict children. The difficulty lies in squaring these facts – which seem documentable only at an intuitive level – with free speech law. The

---

[51] Rimm, "Marketing Pornography," 1890.

[52] Rimm, "Marketing Pornography," 1892.

[53] Catherine Mackinnon, "Vindication and Resistance: A Response to the Carnegie Mellon Study of Pornography in Cyberspace," *Georgetown University Law Journal* 83 (1995), 1962.

[54] Robert Cannon, "The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway," *Federal Communications Law Journal* 49 (1996), n. 4 and n. 25.

[55] Cannon, "Legislative History," 55-56, citations omitted. See also the discussion in Charles Platt, *Anarchy Online*.

Supreme Court took a rather dim view of the CDA, striking down several provisions of the act 7-2 (the two dissents were only partial). The CDA had prohibited all transmission of "indecent" material to minors. The Court severed the indecency restriction from the statute because such a ban against undefined indecency would unduly chill the speech of Internet users. "Indecency," it turns out, is not a legal term. One is entitled to restrict "obscene" speech (*i.e.*, it is not protected by the first amendment), and the Court had articulated a three pronged test to determine if speech was obscene:

> (a) whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.[56]

The CDA's restrictions on "indecent" had no such qualifications attached. The Court wondered aloud: "Could a speaker confidently assume that a serious discussion about birth control practices, homosexuality, the First Amendment issues raised by the Appendix to our *Pacifica* opinion [which allowed restriction of profanity on radio shows], or the consequences of prison rape would not violate the CDA?"[57] Since speech on the net should receive "unqualified" protection, restrictions would have to be subject to strict scrutiny: they would have to serve a compelling governmental interest, they would have to be narrowly tailored to serve that interest, and they would have to be the least intrusive means available to achieve it. The Court expressed skepticism regarding the CDA's ability to meet any part of this standard, in particular the idea that it was "narrowly tailored" to restricting obscene speech, since the statutory text did not even use the word "obscene."

Congress responded by passing the very similar "Child Online Protection Act," which the 3rd Circuit Court of Appeals struck down because the statute's attempt to invoke the "community standards" criteria required by the Supreme Court could not be applied to cyberspace, at least not as written into the law. The Court wrote that "because material posted on the [World Wide] Web is accessible by all Internet users worldwide, and because current technology does not permit a Web publisher to restrict access to its site based on the geographic locale of each particular Internet user, COPA essentially requires that every Web publisher subject to the statute abide by the most restrictive and conservative state's community standards in order to avoid criminal liability."[58] The question of Internet pornography, then, like other questions of computer ethics, is deeply involved in basic questions about the nature of the net. Where is cyberspace? Such questions matter.

Congress has responded to these sorts of setbacks by encouraging, and attempting to mandate in schools and libraries, the use of filtering software.[59] This software works as an attachment to a user's browser, prohibiting access to sites which are on a list maintained by the manufacturer of the software, or which attempt to display content which the filter deems offensive. Filtering software

---

[56] *Reno v. ACLU*, 872; citing *Miller v. California*, 413 U.S. 15 (1973), at 24.

[57] *Reno v. ACLU*, 871.

[58] "3rd Circuit Court Upholds Injunction Against Child Online Protection Act," *The Legal Intelligencer* (June 23, 2000). The act is at 47 USCS §231.

[59] For a discussion of current legislative efforts, see "McCain Renews Porn-Filter Push," *Wired News* (June 27, 2000).

has an intuitive appeal: it seems to operate without government intrusion, and can be updated quickly to keep pace with obscenity online. It also has severe problems. First, if one values free expression and debate, the filtering software can be said to threaten expression even more than an outright prohibition, since a user might not even know that the material is being filtered. Requiring libraries and schools to use filtering programs would thus presumably raise the same free speech issues as the CDA. The programs also do not work perfectly. For example, CYBERsitter changed the sentence "President Clinton opposes homosexual marriage" into "President Clinton opposes marriage."[60] In the wake of his various extramarital excursions, one might be inclined to agree with the latter statement – but the filtered statement is not what was written originally, and a library user would have no way to know this. Other effects of overbroad filtering programs threaten to impede research and to shut down access to speech which the filtering company deems offensive, whether or not it is pornographic:

> Another example of a difficulty with string-recognition software occurred when software utilized by America Online would not let users from 'Scunthorpe,' England, register with the service. Also, Surfwatch software prevented the University of Kansas Medical Center from accessing their own 'Archie R. Dykes Medical Library [sic].' Some companies, like CYBERsitter, filter out gay and lesbian sites even when they do not contain a reference to sex.[61]

The forced imposition of filtering programs, in other words, raises as many questions as it answers.[62] The filtering of gay and lesbian sites becomes particularly troubling, because companies use the copyright statute to prevent users who have not already purchased the software from determining which sites it filters.[63]

One final issue should be raised with respect to computer pornography. This issue is wholly new with the developments in computer technology. Virtually everyone will agree that child pornography, the depiction of children in various kinds of sexual activity, is a bad thing. There are a variety of reasons for this judgment: the children themselves are victimized, and will likely be psychologically scarred for the remainder of their lives; the images encourage pedophiles to abuse additional children, and so forth. The basis of this judgment, then, is an equation of child pornography and child abuse, the belief that children require protection from predatory adults who would engage them in damaging activities they do not even fully understand. Assuming that this judgment is correct (there are those who dispute various aspects of it; it is not necessary here to engage that discussion),

[60] Doherty, "obscenity.com," 297.

[61] Doherty, "obscenity.com," 297, n. 281. Doherty downplays these risks as technologically surmountable.

[62] A federal district court in 1998 rejected, on almost all possible first amendment grounds, the mandatory usage of such filtering software on all library computers. See *Mainstream Loudon v. Board of Trustees of Loudon County Library*, 24 F. Supp. 2d 552 (1998).

[63] As for example the recent decisions against the writers of CPHack. See "Battle Brews over Reverse Engineering," *CNN.com* (May 8, 2000). As this article points out, there is an international issue here: many companies which wish to reverse engineer are establishing operations in Europe, where the DMCA's provisions do not apply.

child pornography poses new problems online. It is not just that its access and distribution becomes easier. It is that computer imaging technology now exists for the creation of "virtual pornography." In such virtual porn, either sexual images of adults or nonsexual images of children (both legal) are "morphed" by computer imaging techniques to create sexual images of children.[64]

The policy question posed is whether such virtual child porn should be banned or not. Congress says that it should, in the Child Pornography Prevention Act of 1996, which expands the definition of child pornography to include that generated by computers under a variety of conditions. The most "virtual" is that it "it depicts, or appears to depict, a minor engaging in sexually explicit conduct."[65] In other words, if it looks like child porn, then it is. The prohibition seems to present a test case for the protection of universally condemned free speech: one of the main reasons that child pornography is prohibited is that its production actually harms children. If no children are involved, or if the children involved are not themselves doing anything sexual, then presumably that reason goes away. As one scholar has shown, absent this actual harm to actual children, many of the other reasons given to prohibit child pornography are a difficult fit with judicial decisions protecting offensive speech.[66] In other words, the development of virtual reality technology brings to the fore the reasons behind our ethical judgments concerning, for example, child pornography and free speech.

In sum: in addition to raising all of the difficult questions surrounding all other forms of pornography, the question of online pornography raises numerous other issues related to computers: how does one understand geography in cyberspace? How do various computer laws interact? How does one determine what "computer pornography" *is*? Who should get to make these decisions? None of these issues are going away.

---

[64] See Debra D. Burke, "The Criminalization of Virtual Child Pornography: A Constitutional Question," *Harvard Journal on Legislation* 34 (Summer 1997), 440-441.

[65] Burke, "Virtual Child Pornography," 441.

[66] Burke, "Virtual Child Pornography," *passim.* That said, Burke's suggestion – that tort law (depiction in a false light because nonsexual images are made sexual) could protect children from unauthorized morphing of their images - seems crazy in this context: how could a child know that his or her image had been used for child pornography, unless he or she had been viewing such pornography?

SELECT BIBLIOGRAPHY

The following bibliography does not include news articles. It is divided into articles/books, and court decisions.

Works Cited: Articles and Books

"An Appraisal of the Technologies of Political Control." STOA Interim Study, Sept. 1998, http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm.

Association for Computing Machinery. "Code of Ethics for Software Engineers," at URL: http://www.acm.org/serving/se/code.htm.

Aoki, Keith. "Considering Multiple and Overlapping Sovereignties: Liberalism, Libertarianism, National Sovereignty, 'Global' Intellectual Property, and the Internet." *Independent Journal of Global Legal Studies* 5 (Spring 1998), 443-473.

Balibar, Étienne. "*Sujet, individu, citoyen. Qu'est-ce que 'l'homme' au XVIIe siècle?*" In *L'individu dans la théorie politique et dans la pratique*, ed. Janet Coleman. Paris: PUF, 1996, 249-277.

Barlow, John Perry. "A Declaration of the Independence of Cyberspace" (1996) at URL: http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration.

Barwise, Jon and John Etchemendy. "Digital Metaphysics." In Terrell Ward Bynum and James H. Moor, eds., *The Digital Phoenix: How Computers are Changing Philosophy.* Oxford: Blackwell, 1998, 117-134.

Bayles, Michael D., ed. *Contemporary Utilitarianism.* New York: Anchor Books, 1968.

Benhabib, Seyla. "The Generalized and the Concrete Other: The Kohlberg-Gilligan Controversy and Feminist Theory." *Praxis International* 5 (1986), 402-424.

Benjamin, Stuart Minor. "Stepping into the Same River Twice: Rapidly Changing Facts and the Appellate Process." *Texas Law Review* 78:2 (December 1999), 269-373.

Bentham, Jeremy. "Panopticon Papers" In *A Bentham Reader*, ed. Mary Peter Mack . New York: Pegasus, 1969.

Berghel, Hal. "Identity Theft, Social Security Numbers, and the Web." *Communications of the ACM* (February. 2000), 17.

Bork, Robert H. *The Tempting of America: The Political Seduction of the Law.* New York: Free Press, 1990.

Boyle, James. *Shamans, Software and Spleens*. Cambridge, Mass: Harvard UP, 1996.

Burk, Dan L. "Muddy Rules for Cyberspace." *Cardozo Law Review* 21 (1999), 121-179.

Burke, Debra D. "The Criminalization of Virtual Child Pornography: A Constitutional Question." *Harvard Journal on Legislation* 34 (Summer 1997), 339-472.

Butler, Judith. *Excitable Speech*. London: Routledge, 1997.

Bynum, Terrell Ward. "Global Information Ethics and the Information Revolution," in Terrell Ward

Bynum, Terrell Ward and James H. Moor. "How Computers are Changing Philosophy," in Terrell Ward Bynum and James H. Moor, eds. *The Digital Phoenix: How Computers are Changing Philosophy.* Oxford: Blackwell, 1998, 1-14.

Cannon, Robert. "The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway." *Federal Communications Law Journal* 49 (1996), 51-94.

Cohen, Julie E. "Copyright and the Jurisprudence of Self-Help." *Berkeley Technology Law Journal* 13 (Fall 1998), 1089-1143.

-----. "Lochner in Cyberspace: The New Economic Orthodoxy of 'Rights Management.'" *University of Michigan Law Review* 97 (November, 1998), 462-563.

-----. "A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace," *Connecticut Law Review* 28 (Summer, 1996), 981-1039.

Conley, John M. *et. al.* "Database Protection in a Digital World." *Richmond Journal of Law and Technology* 6:2 (Symposium 1999), at URL: http://www.richmond.edu/jolt/v6i1/conley.html

Crenshaw, Kemberle. "Gender, Race, and the Politics of Supreme Court Appointments." *Southern California Law Review* 65 (March, 1992), 1467-1476.

Denning, Peter J. "The Internet after Thirty Years." In Peter J. Denning and Dorothy E. Denning, eds., *Internet Besieged: Countering Cyberspace Scofflaws*. New York: ACM Press, 1998, 15-28.

Descartes, Rene. *Discourse on the Method*, in *The Philosophical Writings of Descartes*. trans. John Cottingham, Robert Stoothoff and Dugald Murdoch. Cambridge: Cambridge UP, 1985, I:116-117.

Devins, Neal. "Review Essay: Judicial Matters: The Hollow Hope: Can Courts Bring About Social Change?" *California Law Review* 80 (July 1992), 1027-1069.

Dibble, Julian. "A Rape in Cyberspace." *Village Voice* (December 23, 1993), at URL: http://www.levity.com/julian/bungle_vv.html.

Doherty, Kelly M. "www.obscenity.com: An Analysis of Obscenity and Indecency Regulation on the Internet." *Akron Law Review* 32 (1999), 259-300.

Dworkin, Ronald. *Taking Rights Seriously*. Cambridge, Mass: Harvard UP, 1977.

Eskridge, William. *Dynamic Statutory Interpretation*. Cambridge, Mass: Harvard UP, 1994.

Etzioni, Amitai. *The Limits of Privacy*. New York: Basic Books, 1999.

Floridi, Luciano. "Information Ethics: On the Philosophical Foundation of Computer Ethics," at URL: http://www.wolfson.ox.ac.uk/~floridi/ie.htm.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan. New York: Vintage Books, 1977.

Garon, Jon M. "Media & Monopoly: Slowing the Convergence at the Marketplace of Ideas." *Cardozo Arts and Entertainment Law Journal* 17:491 (1999), 491-621.

Gershenfeld, Neil and Isaac L. Chuang, "Quantum Computing with Molecules." *Scientific American* (June 1998), at URL: http://www.sciam.com/1998/0698issue/0698gershenfeld.html

Gewirth, Alan. "Are There Any Absolute Rights?" in *Human Rights: Essays on Justification and Applications*. Chicago: U. Chicago Press, 1982, 218-233.

-----. "Can Utilitarianism Justify any Moral Rights?" in *Human Rights*, 143-162.

Gindin, Susan E. "Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet." *San Diego Law Review* 37 (1997), 1153-1223.

Glass, Brett. "Keeping your Private Information Private," *PC Magazine* (July 21, 2000 [reedited]), at URL: http://www.zdnet.com/pcmag/stories/reviews/0,6755,2572515,00.html.

Glendon, Mary Ann. *Rights Talk : The Impoverishment of Political Discourse*. New York: Free Press, 1991.

Godwin, Mike. "Net to Worry," *Communications of the ACM* 42:12 (December 1999), 16.

Goldman, Alan. *The Moral Foundations of Professional Ethics*. Totowa, NJ: Rowan and Littlefield, 1980.

Gotterbarn, Don, Keith Miller and Simon Rogerson. "Software Engineering Code of Ethics is Approved." *Communications of the ACM* 42:10 (October 1999), 102-107.

Hare, R. M. "Rights, Utility, and Universalization: Reply to J.L. Mackie." In *Utility and Rights*, ed. R. G. Frey. Minneapolis: University of Minnesota Press, 1984, 106-120.

Hatcher, Michael, Jay McDannell and Stacy Ostfeld. "Computer Crimes." *American Criminal Law Review* 36 (Summer 1999), 397-444.

Haynes, Mark A. "Black Holes of Innovation in the Software Arts." *Berkeley Technology Law Journal* 14:567 (Spring 1999), 567-575.

Heller, Michael A. "The Tragedy of the Anticommons: Property in the Transition from Marx to Markets." *Harvard Law Review* 111 (1998), 621-688.

Hobart, Michael E. and Zachary S. Schiffman. *Information Ages: Literacy, Numeracy, and the Computer Revolution*. Baltimore: Johns Hopkins UP, 1998.

Hodges, Michael P. "Does Professional Ethics Include Computer Professionals? Two Models for Understanding." In *Computers and Ethics in the Cyberage*, ed. D. Micah Hester and Paul J. Ford. Upper Saddle River, NJ: Prentice Hall, 2001.

Howe, Jeff. "Copyrighting the Book of Life." *Feed* (April 12, 2000), at URL: http://www.feedmag.com/dna/bookoflife.html.

Hull, Gordon. "On the Fetishization of Cyberspeech and Turn from 'Public' to 'Private' Law." *Philosophy and Social Criticism* (under consideration).

Introna, Lucas D. "Privacy and the Computer: Why We Need Privacy n the Information Industry." *Metaphilosophy* (1997).

Johnson, Deborah G. *Computer Ethics*. Upper Saddle River, NJ: Prentice Hall, 1994.

Jones, James A. "The Immigration Marriage Fraud Amendments: Sham Marriages or Sham Legislation?" *Florida State University Law Review* 24 (Spring 1997), 679-701.

Joy, Bill. "Why the future doesn't need us." *Wired* (April 2000), at URL: http://www.wired.com/wired/archive/8.04/joy_pr.html.

Kant, Immanuel. *Critique of Practical Reason*, trans. Mary Gregor. Cambrdige: Cambridge UP, 1997.

-----. *Foundations of the Metaphyiscs of Morals*, trans. Lewis White Beck. New York: MacMillan, 1990.

Law, Sylvia A. "Homosexuality and the Social Meaning of Gender." *Wisconsin Law Review* (1988), 187-235.

Lee, Donna R. "Mail Fantasy: Global Sexual Exploitation in the Mail-Order Bride Industry and Proposed Legal Solutions." *Asian Law Journal* 5 (May 1998), 139-179.

Lee, Michael, *et. al.* "Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal." *Berkeley Technology Law Journal* 14 (Spring, 1998), 839-886.

Lessig, Lawrence. *Code and other Laws of Cyberspace*. New York: Basic Books, 1999.

Litman, Jessica. "Electronic Commerce and Free Speech," at URL: http://papers.ssrn.com/paper.taf?ABSTRACT_ID=218275

Locke, John. Second *Treatise on Government.* In *The Works of John Locke* IV. London, 1824.

Lycan, William G. "Response to my Critics." In Terrell Ward Bynum and James H. Moor, eds. *The Digital Phoenix: How Computers are Changing Philosophy*. Oxford: Blackwell, 1998.

Macedo, Stephen. "Originalism and the Inescapability of Politics." *Northwestern University Law Review* 84 (1990), 1203-1214.

MacIntyre, Alasdair. *After Virtue: A Study in Moral Theory*. Notre Dame, IN: U. of Notre Dame Press, 1984).

Mackie, J. L. "Rights, Utility, and Universalization." In *Utility and Rights*, ed. R. G. Frey. Minneapolis: University of Minnesota Press, 1984, 86-105

MacKinnon, Catherine. *Feminism Unmodified: Discourses on Life and Law* (Cambridge, Mass: Harvard UP, 1987).

-----. "Reflections on Sex Equality Under Law." *Yale Law Journal* 100 (1991), 1281-1328.

-----. "Vindication and Resistance: A Response to the Carnegie Mellon Study of Pornography in Cyberspace." *Georgetown University Law Journal* 83 (1995), 1959-1967.

McManis, Charles R. "The Privatization (or 'Shrink-Wrapping') of American Copyright Law." *California Law Review* 87 (1999), 173-190.

Mill, J. S. *Utilitarianism.* Indianapolis, IN: Hackett, 1979.

Moor, James H. "What is Computer Ethics?" *Metaphilosophy* 16:4 (October 1985), 266-275.

National Public Radio, Kaiser Family Foundation and Harvard University. *Computer Use Survey* (February 2000), at URL: http://www.npr.org/programs/specials/poll/technology/index.html

Nietzsche, Friedrich. *Beyond Good and Evil*, in *Basic Writings of Nietzsche*, trans. Walter Kaufmann. New York: The Modern Library, 1966.

Nimmer, David, Elliot Brown and Gary N. Frischling. "The Metamorphosis of Contract into Expand." *California Law Review* 87 (1999), 17-77.

Penner, J. E. "The 'Bundle of Rights' Picture of Property." *UCLA Law Review* 43 (February 1996), 711-820.

Pippin, Major R. Ken. "Consumer Privacy on the Internet: It's 'Surfer Beware.'" *Air Force Law Review* 47 (1999), 125-161.

Platt, Charles. *Anarchy Online*. New York: Harper Prism, 1996.

Pooley, Sam. "The State Rules, OK? The Continuing Political Economy of Nation-States." *Review of Radical Political Economics* 22:1 (1990), 45-58.

Rimm, Marty. "Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in over 2,000 Cities in Forty Countries, Provinces, and Territories," *Georgetown University Law Journal* 83 (1995), 1849-1934.

Rosenberg, Gerald N. *The Hollow Hope.* Chicago: U. Chicago Press, 1991.

Samuelson, Pamela. "Why the Anti-Circumvention Regulations Need Revision." *Communications of the ACM* 42:9 (September, 1999), 17-21.

Schneier, Bruce. "Risks of Relying on Cryptography." *Communications of the ACM* 42:10 (October, 1999), 144.

Schuck, Peter H. "Book Review: Public Law Litigation and Social Reform." *Yale Law Journal* 102 (May 1993), 1763-1786.

Shrader-Frechette, Kristin. *Risk and Rationality*. Berkeley: U. California Press, 1991.

Spafford, Eugene. "Are Computer Hacker Break-ins Ethical?" In Peter J. Denning and Dorothy E. Denning, eds., *Internet Besieged: Countering Cyberspace Scofflaws*. New York: ACM Press, 1998, 493-506.

Stallman, Richard. "Why Software Should not Have Owners," at URL: http://www.draper.net/gnu/philosophy/why-free.html.

Sumner, L. W. "Rights Denaturalized." In *Utility and Rights*, ed. R. G. Frey. Minneapolis: University of Minnesota Press, 1984, 20-41.

Swire, Peter P. "Of Elephants, Mice, and Privacy: International Choice of Law and the Internet." At URL: http://papers.ssrn.com/paper.taf?ABSTRACT_ID=121277.

Toulmin, Stephen. *The Uses of Argument*. Cambridge: Cambridge UP, 1958.

United States Copyright Office. See "The Digital Millenium Copyright Act of 1998: U.S. Copyright Office Summary" (December, 1998), at URL: http://lcweb.loc.gov/copyright/legislation/dmca.pdf.

United States Department of Commerce. *Digital Economy 2000*, at URL: http://www.esa.doc.gov/de2k.htm.

United States Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 25, 2000), at URL: http://www.ftc.gov/os/2000/05/testimonyprivacy.htm.

Upham, Frank K. "Unplaced Persons and Movements for Place." In *Postwar Japan as History*, ed. Andrew Gordon. Berkeley: University of California Press, 1993, 325-346.

Urmson, J. O. "The Interpretation of the Moral Philosophy of J. S. Mill," in Michael D. Bayles, ed. *Contemporary Utilitarianism*. New York: Anchor Books, 1968, 13-24.

Warren, Samuel D. and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4:5 (1890), 193-220.

Whitaker, Reg. *The End of Privacy: How Total Surveillance is Becoming a Reality*. New York: The New Press, 1999.

Winterson, Jeanette. "My name is my dot-com." *The Times (London)* (March 29, 2000).

Wolfson, Joel Rothstein. "Contract and Copyright are Not at War." *California Law Review* 87 (1999), 79-110.

Zaner, Richard M. *Troubled Voices: Stories of Ethics and Illness*. Cleveland, Ohio: Pilgrim Press, 1993.

Works Cited: Court Decisions

Amazon.com v. Barnesandnoble.com, 73 F. Supp. 2d 1228 (WD Wa, 1999).

Apple v. Franklin, 714 F 2d 1940 (3CA 1983).

Bobbs-Merrill Co. v. Straus, 210 US 339 (1908).

Bowers v. Hardwick, 478 US 186 (1986).

Brookfield v. West Coast Entertainment, 174 F.3d 1036 (9CA, 1999).

CompuServe v. Patterson, 89 F.3d 1257 (1996), 1263.

Deshaney v. Winnebago, 498 U.S. 189 (1989).

Diamond v. Diehr, 101 S.Ct. 1048 (1981).

Eisenstadt v. Baird, 405 U.S. 438 (1972).

Feist v. Rural Telephone, 499 US 340 (1991).

Griswold v. Connecticut, 381 US 479 (1965).

In re Schrader, 22 F.3d 290, 292 (Fed. Cir. 1994).

Junger v. Daley, 209 F.3d 481 (6CA 2000).

Lochner v. New York, 198 U.S. 45 (1905).

Mainstream Loudon v. Board of Trustees of Loudon County Library, 24 F. Supp. 2d 552 (1998).

Miller v. California, 413 U.S. 15 (1973).

Mink v. AAAA Development, 190 F.3d 333 (1999), 337.

Planned Parenthood v. Casey, 505 U.S. 833 (1992).

Playboy v. Netscape, 55 F. Supp. 2d 1070 (CD Ca, S. Div., 1999).

Qualitex v. Jacobsen Products, 514 U.S. 159 (1995).

Quokka, No. C-99-5076-DLJ (ND Ca, Dec. 13, 1999).

Reno v. ACLU, 521 U.S. 844 (1997).

Roe v. Wade, 410 U.S. 113 (1973).

Santa Fe Independent School District v. Doe, No. 99-62 (June 19, 2000). Available online at: http://www.usscplus.com/current/cases/PDF/9900081.pdf.

Stanley v. Georgia, 394 U.S. 557 (1969).

State Street Bank v. Signature Financial Group, 927 F. Supp. 502 (1996), 26.

U.S. v. Kennedy, 81 F. Supp. 2d 1103 (USD Kansas, 2000).

U.S. v. LaMacchia, 871 F. Supp. 535 (USD Mass, 1994).

U.S. v. Microsoft, Conclusions of Law (April, 2000).

U.S. v. Thomas, 74 F.3d 701 (1996).

Universal City Studios v. Reimerdes, 82 F. Supp. 2d 211 (SD NY, 2000).

Universal Cities v. Reimerdes, 00 Civ. 0277 (LAK) (July 17, 2000).

University of Texas v. Camenisch, 451 U.S. 390.

Whelan Associates v. Jaslow Dental Laboratory, Inc., 609 F.Supp. 1307 (EDPa 1985), affirmed 797 F.2d (3CA 1986).

Zippo Manufacturing Co. v. Zippo Dot Com, 952 F. Supp. 1119 (WD Pa).