Moral Enterprise

Wherever rules are created and applied, we should be alive to the possible presence of an enterprising individual or group. Their activities can properly be called moral enterprise, for what they are enterprising about is the creation of a new fragment of the moral constitution of society, its code of right and wrong. (Becker 1963: 145)

The story of the creation of this 'social menace' is central to the ongoing attempts to rewrite property law in order to contain the effects of the new information technologies that, because of their blindness to the copyrighting of intellectual property, have transformed the way in which modern power is exercised and maintained. (Ross 1991:80 & 81)

Professional ethos

The most prominent hacker crossover success-and-failure was that of Comsec Data Security, a Houston consulting firm founded
in 1991 by three former members of the Legion of Doom. Though the firm quickly built a client list that included several Fortune 500 companies, "media hysteria" and "blackballing" by competing Establishment firms cost the firm those same commissions and forced it out of business in 1992, says cofounder and former president Christopher Goggans. "There are a large number of people who would kill to do nothing but get paid to hack legitimately, so everybody in the hacker community was watching Comsec," says Goggans. "From the treatment we got, you can expect that hackers who want to sell their skills as information security consultants in the future are going to have to hide their backgrounds." (Roush 1995:6)

Commercially-minded hype

It's very hard getting facts … because the media hype is used as a trigger by people who are trying to sell anti-virus devices, programs, scanners, whatever. This is put about very largely by companies who are interested in the market and they try to stimulate the market by putting the fear of God into people in order to sell their products, but selling them on the back of fear rather than constructive benefits, because most of the products in the industry are sold on constructive benefits. You always sell the benefit first, this is selling it on the back of fear which is rather different, "you'd better use our products or else" (Taylor: Knutsford interview).

Viral Hype

software vendors are now profiting from the new public distrust of program copies ... the effects of the viruses have been to profitably clamp down on copyright delinquency, and to generate the need for entirely new industrial production of viral suppressors to contain the fallout. In this respect it is hard to see how
viruses could hardly, in the long run, have benefited industry producers more. (Ross 1990: 80).

Peas in a Pod?

Ironically, these hackers are perhaps driven by the same need to explore, to test technical limits that motivates computer professionals; they decompose problems, develop an understanding of them and then overcome them. But apparently not all hackers recognise the difference between penetrating the technical secrets of their own computer and penetrating a network of computers that belong to others. And therein lies a key distinction between a computer professional and someone who knows a lot about computers. (Edward Parrish 1989).

Shared qualities

Zenner and Denning[1] alike discussed the nature of *Phrack's* articles. They found that the articles appearing in *Phrack* contained the same types of material found publicly in other computer and security magazines, but with one significant difference. The tone of the articles. An article named 'How to Hack Unix' in Phrack usually contained very similar information to an article you might
see in Communications of the ACM only to be named 'Securing Unix Systems'. (Craig Neidorf: CuD 2.07).

Pot, kettle, black

Any computer undergrounder can identify with and appreciate Stoll's obsession and patience in attempting to trace the hacker through a maze of international gateways and computer systems. But, Stoll apparently misses the obvious affinity he has with those he condemns. He simply dismisses hackers as 'monsters' and displays virtually no recognition of the similarities between his own activity and those of the computer underground. This is what makes Stoll's work so dangerous: His work is an unreflective exercise in self-promotion, a tome that divides the sacred world of technocrats from the profane activities of those who would challenge it; Stoll stigmatises without understanding (Thomas 1990).

Degradation ritual

Stoll … labels hackers as "monsters" despite the fact he shares some of their qualities illustrates the rhetorical qualities of the computer security industry's boundary forming process. This is called a degradation ritual which aims at redefining the social acceptability of a group by using assertion and hyperbole in the place of reasoned argument. Thus Stoll refers periodically in his book to hackers as "rats, monsters, vandals, and bastards" (cited in Thomas 1990)

Witch-hunts and hackers

The kinds of practices labelled deviant correspond to those values on which the community places its highest premium. Materialist cultures are beset by theft (although that crime is meaningless in a utopian commune where all property is shared) ... The correspondence between kind of deviance and a community's salient values is no accident ... deviants and conformists both are shaped by the same cultural pressures -- and thus share some, if not all, common values -- though they may vary in their opportunities to pursue valued ends via legitimate means. Deviance ... emerges exactly where it is most feared, in part because every community encourages some of its members to become Darth Vader, taking 'the force' over to the 'dark side' (Dougan and Gieryn 1990: 4).

Cold War mentality

John Perry Barlow identifies the hacker as the latest such scapegoat of modern times in a series including Communism, terrorism, child abductors and AIDS. He sees post Cold War feelings of vulnerability and the information/generation gap being constitutive factors in the witch-hunt mentality:

More and more of our neighbours live in armed compounds. Alarms blare continuously. Potentially happy people give their lives over to the corporate state as though the world were so dangerous outside its veil of collective immunity that they have no choice ... The perfect bogeyman for modern times is the Cyberpunk! He is so smart he makes you feel even more stupid than you usually do. He knows this complex country in which you're perpetually lost. He understands the value of things you can't conceptualize long enough to cash in on. He is the one-eyed man in the Country of the Blind (Barlow 1990: 56).

---

[1] The former was the defence lawyer for Craig Neidorf in the E911 trial of 1990, Dorothy Denning is a computer scientist from Georgetown University, Washington, with an academic interest in computer underground issues.

The hardening of attitudes

Computer crimes have evolved from exotic incidents to a major societal issue. They have quickly moved from hacks to attacks, from fooling around to fouling up, and from violations to virucide. In order to fight computer crime, the society, and computer professionals in particular, face some very difficult decisions on some very fundamental issues. This is a serious moment in our society, as we seek to establish an appropriate balance between old law and new technology. (Sherizen 1992: 39)

Wannabe's – qty & quality

1989 hacker movie Wargames:

In a matter of months the number of self-proclaimed hackers tripled, then quadrupled. You couldn't get through to any of the old bulletin boards any more - the telephone numbers were busy all night long. Even worse, you could delicately work to gain entrance to a system, only to find dozens of
novices blithely tromping around the files. (Landreth 1985 :18).

Loss of community spirit

People were friendly, computer users were very social. Information was handed down freely, there was a true feeling of brotherhood in the underground. As the years went on people became more and more anti-social. As it became more and more difficult to blue-box the social feeling of the underground began to vanish. People began to hoard information and turn people in for revenge. The underground today is not fun. It is very power hungry, almost feral in its actions. People are grouped off: you like me or you like him, you cannot like both ... The subculture I grew up with , learned in, and contributed to, has decayed into something gross and twisted that I shamefully admit connection with. Everything changes and everything dies, and I am certain that within ten years there will be no such thing as a computer underground. I'm glad I saw it in its prime (Goggans: email interview).

Sheer numbers

The idiosyncratic actions of the first generation hackers, within the isolated academic context of MIT, were often praised for their inventiveness. Similar actions in the wider modern computing community tend to be automatically more disruptive and liable to censure. Once the prototype days of a technology are over, society's investment in the technology makes cavalier attitudes by figures such as hackers, increasingly unacceptable.

Pioneering Days

… historical change shows how certain individual behaviours become changed by societal restructuring … These barnstormers were wild, didn't respect property, and were constantly challenging authority. When they crashed their system, it really went down. They were a unique breed of individuals, who tested the limits of the world of aviation, sometimes literally by walking on the wings and performing amazing and often dangerous stunts. They were necessary for the early stages of aviation because they tested the limits of the technology … What finally led to the end of the barnstorming pilots was that the business interests of airlines got precedence over the aviation interests … After the industry reached a certain level of development, these "pilot hackers" could have quite literally killed the industry … certain deviant behaviors get resolved, often without changing the behavior but by creating an institutionalized patterning, accepting certain activities and sidetracking other behaviors. There will be a process that will challenge the computer crime problem. It will not necessarily be the same as with airline pilots but it will be a process whereby at least a temporary resolution will be reached. (Sherizen 1992: 43)

Pioneering cont

When the first 'airplane hackers' began working on their devices, they were free to do essentially as they pleased. If they crashed and killed themselves well, that was too bad. If their planes worked - so much the better. After it became possible to build working airplanes, there followed a period in which anyone could build one and fly where he liked. But in the long run that became untenable ... If you want to fly today, you must get a license. You must work within a whole set of regulations. (Jerry Leichter: CuD 4.18).

Pressures to criminalise

The law-makers have endorsed that schizophrenia pressed by the electro-cognoscenti, and they have endorsed it out of fear, ignorance and misunderstanding. How else to react to the omniscient, omnipotent power of cyberspace? Well, take its unruly tenants at their word [they seem to know what they are talking about], and treat cyberspace as a competing reality: regulate it, and break it up into chunks called property. But alternative universes provide a very bad model: Neither law nor technology benefits. The law founders and sinks in the clear blue fungible sea of the network. And the electronic community is on the verge of being legislated to death, ruled out of fear and loathing, chained by broad and detailed laws that can make anything -- the movement of an electron—illegal. (Karnow 1994: 7-8)

Pressure to legislate

We should not be surprised by computer crime, but we seem to be. In *The Great Train Robbery* Michael Crichton suggested that society is often offended by this new technology crime to the point of outrage. Likewise, it should come as little surprise, that, like the railroad, the automobile, and the telephone before it, the computer has been the subject of premature, if not pre-emptive, legislation. The politicians are certain, that, somewhere in any dung heap, there must be a pony. (Murray 1992: 31)

I would like to criticise the press in its handling of the 'hackers', the 414 gang, the Dalton, gang etc. The acts performed by these kids are vandalism at best and probably trespass and theft at worst. It is only the inadequacy of the criminal code that saves the hackers from very serious prosecution. The companies that are vulnerable to this activity, (and most large companies are very vulnerable) are pressing hard to update the criminal code. (Thompson 1984: 763).

Legislation

Through legislation we can turn what the hackers do into a crime and there just might be a slim chance that we can stop them. But that won't fix poorly designed systems whose very existence is a violation of our privacy. (Goldstein 1993).

We now face the task of adapting our legal institutions and societal expectations to the cultural phenomena that even now are springing up from communications technology. (Kapor 1991:1)

The law only has sledgehammers, when what we need are parking tickets and speeding tickets - Mitch Kapor (Cited in Sterling 1991:6).

Problems with legislation

1) it will not succeed in eliminating hacking and as such can be described as 'symbolic legislation'

2) it will increase the likelihood that existing security weaknesses will shelter behind the law and remain unrectified

3) and a potential problem associated with even successfully implemented legislation is the danger of driving hacking knowledge into the hands of the criminal fraternity.

General problem – pace of change & ambivalent commodity status of info

Information as property?

I think it stems from the cultural (in a sociological sense) basis which we use to attach financial values to things. Cars and houses have a financial and personal value which most people can negotiate and agree on. If we suffer loss or damage to this kind of object we can usually gauge that loss and society can work out some recompense for that loss (insurance, punishing offenders etc.) I think information, especially electronic information is different. We don't have the necessary agreed mechanisms on which to establish its financial and personal value. By its very nature it is very easy to move ('steal'). Thus given the lack of effort in 'stealing' it and the lack of any perceived damage (on behalf of the thief) it is not seen (by them) as a real crime (Dr David England Glasgow University: email interview).

Technocracy & information

In this context, hackers fail to perceive much of their activity as a crime. They see the new emphasis being deliberately placed upon ethics in the professional worlds of business and science as part of an attempt to develop a coherent response to the contradictions associated with information's evolving nature: “For all the trumpeting about excesses of power and disrespect for the law of the land, the revival of ethics, in the business and science disciplines in the Ivy League and on Capitol Hill ... is little more than a weak liberal response to working flaws or adaptational lapses in the social logic of technocracy" (Ross, 22: 1990).

Symbolic Legislation

Lobbying by computer users for the criminalisation of cruelty to (their) computers has been extensive and vociferous. The imposition of criminal sanctions is seen as some sort of magic talisman ... the law takes the computer too seriously. All sorts of magical qualities are ascribed to the machine. The debates on the Computer Misuse Act are replete with demonic images of hacking and its consequences. The computer is the ultimate bogeyman and has produced a knee jerk reaction from Parliament (Ian Lloyd- Strathclyde University Law Department, 9. 6.1993: Edinburgh University AI Dept. Seminar).

Symbolic Legislation

While the Computer Fraud and Abuse Act has been amended several times, it still does not cover every conceivable computer crime. Therefore it is imperative that legislators continue to amend the Act, as well as pass other criminal statutes, as the technology and scope of computer crime expands. Without such statutes, law enforcement agencies and prosecutors will be handcuffed in their efforts to combat this new generation of computer criminals. As one commentator points out, "The revolution has
only just begun, but already it's starting to overwhelm us. It's outstripping our capacity to cope, antiquating our laws, transforming our mores, reshuffling our economy, reordering our priorities, redefining our workplaces, and putting our Constitution to the fire. (Scalione 1996:6)

Symbolic Legislation

the unexpressed understanding [of legislators] that unless computer-resident information was extended the ideological and practical protection of the law, established relations of property and hegemonic authority relations could be deroutinised by 'information thieves' ... It was within this ideological framework that the dangers of computer crime proclaimed by computer security experts and the press made sense. And in the final analysis, it was this ideological framework that made the passage of computer crime laws a low-risk, high visibility opportunity for law-makers (Michalowski and Pfuhl, 1990: 271).

Symbolic Legislation

Legislation will at least raise the profile of computer security. Enforcement will be another question ... Nobody can deny the potential and actual threat of hacking. The Law can serve as one plank in its prevention and deterrrence. Increasingly the law is giving out clear signals. It is too early to judge the impact of this ... [but] one cannot but wonder if hacking will prove as intractable as the drugs and Aids issues, and whether the legal response will be as effective as King Canute trying to beat back the waves (Vinten 1990:15).

Instrumental Legislation

the computer industry will welcome the Bill because it cannot build into its technology the necessary safeguards to prevent hacking or other offences. At the moment such safeguards are technically impossible and, therefore, the law must fill the gap (Mr Hogg MP Hansard 1990a: 1143).

Blame displacement

In my view, a computer system that is not properly secure can potentially cause more damage than a
Rambo maniac who gets hold of guns, horrific though that is. Logic surely dictates that computer owners should be legally responsible for the security of their computers just as gun owners are responsible for their guns (Hansard Standing Committee C 1990b: 88).

Instrumental legislation

Legislation was introduced in the context of an apparent unwillingness of companies to invest sufficiently in security measures: "It could be argued that perhaps one fifth of investment in a computer software system should be allocated to security. Very few companies adopt that principle" (Nicholson, Hansard 88: 1990b). Legislation was thus a cost-effective countermeasure with which to confront an otherwise expensive problem:

In much the same way as we lock our doors to deter burglars, it is possible to protect computers, and many people do ... However, there is no complete form of protection for computers. High levels of security can be achieved but they are horrifically expensive, in terms of money, inconvenience or both. Security systems tend to slow up the computer. When speed is the essence, that can be extremely costly. We do not expect householders to turn their homes into Fort Knox. We expect them to take sensible precautions and we add to that the support of sound laws against burglary. That is precisely my approach in the Bill (Mr Colvin MP Hansard 1990a: 1139).

Security thru obscurity

A study of 20 European companies carried out by Coopers and Lybrand showed that 19 had inadequate standards of security which were a real threat to the economic development of those companies. The report said: 'The catastrophic effects of poor security are likely to discourage organisations from becoming any more dependent on their network systems.' That suggests that *there may be a level of complexity in our society beyond which, because of safety interests, we may be frightened to go*. If hacking increases our fears, there will be damage to the cohesion and organisation of our society. That is a perfectly good and sufficient justification for the Bill (Mr Arbuthnot MP Hansard 1990a: 1179 [emphasis mine).

Symbolic deterrence

a characteristic of symbolic legislation (and to a lesser extent most legislation): that it should espouse a particular social message irrespective of the law's likely ability to enforce that message:

It may deter the occasional recreational hacker, but the seriously disturbed person who perpetrates serious offences may not be adequately deterred by it. People will not be deterred if there seems little chance of being caught ... Will inventive minds find some way of circumventing the Bill? I hope that it's drafting is secure enough to prevent that. I support the Bill in principle. Its internal structure is sound, but it is a matter of conjecture whether it will do what it is purported to do (Moonie Hansard 1990a:1160).

Symbolic Legislation

Arguably, any need to deter abuse existed long before the enactment of computer crime statutes. In fact, the available data suggest that serious economic losses linked to computer abuse have been and continue to be attributed to current and former employees of the victimised organisation rather than to interloping hackers with modems. The temporal lag in the criminalisation of computer abuse (not
observed with the introduction of other technological changes), seriously challenges the extent to which the computer crime laws can be understood purely as instruments of classical deterrence (Hollinger and Lanza-Kaduce 1988:116).

Deterrence

Paul Bedworth - two of his co-defendants were sentenced to prison terms. The judge :

If your passion had been cars rather than computers we would have called your conduct delinquent, and I don't shrink from the analogy of describing what you were doing as intellectual joy-riding ... There may be people out there who consider hacking to be harmless, but hacking is not harmless. Computers
now form a central role in our lives ... Some, providing emergency services, depend on their computers to deliver those services. It is essential that the integrity of those systems should be protected and hacking puts that integrity into jeopardy'. He said that hackers need to be given a 'clear signal' by the court that their activities 'will not and cannot be tolerated' (The Independent pg4, Saturday 22 May 1993).

Moral entrepreneurs & degradation ritual

The prototype of the rule creator … is the crusading reformer. He is interested in the content of rules. The existing rules do not satisfy him because there is some evil which profoundly disturbs him. He feels that nothing can be right in the world until rules are made to correct it. He operates with an absolute ethic; what he sees is truly and totally evil with no qualification. Any means is justified to do away with it. The crusader is fervent and righteous, often self-righteous. (Becker 1963: 148)

Old Boy's Club (Them & Us)

Yesterday I received a letter from a constituent who is a leading official in one of the world's leading banks. He asked me to support the Bill, and I am happy to assure him that I do so with enthusiasm ... When such an important official troubles to write to a Member of Parliament about a specific piece of legislation, knowing the background of his career I have not the slightest doubt that the menace of hacking and its consequences is widespread (Powell, Hansard 1990a: 1147).

Old Boy's Club (Them & Us)

To show the sort of twisted culture that the Bill is trying to stamp out, I have an extract from a bulletin board ... stating: 'who's seen the news in the 'Sunday Times' ... page A5 ... about hacking ... and phreaking Mercury ... they also want restrictions on BBS's ... it's that stupid cow ... the Devon MP 'computer expert' [Nicholson] ... don't make me laff ... could be bad news tho ... maybe someone should assassinate her?' Did somebody suggest that hacking is a harmless culture? All that I can say is that it is a privilege and I am honoured to join my hon. Friend on the hackers' hit list (Colvin, Hansard 1990a: 1137).

Nicholson

… describes in detail various salacious and potentially destabilising aspects of hacking activity ranging from proliferation of pornography on bulletin boards to interest being shown by political groups such as the Greens, Anarchists and those behind the 'Electronics and Computing for Peace Newsletter'. She seeks to distance herself from "people who believe that they have a right of access to all knowledge and that everything should be out in the open - and should specifically be open to them". Nicholson proceeds to relate reported incidents of hackers who have allegedly 'tried to kill patients in hospital by accessing their drug records and altering their prescriptions on computer' (Hansard 1990a:1151 + 1153).

Nicholson

It is no good saying that people must increase their protection, because hackers are very clever. They will find a way around every form of protection that one buys or creates. That is what they are there for. They make a great deal of money out of it and the German hackers, at any rate, support a drug-based lifestyle on their activities. I was about to say, 'enjoy', but I should certainly not enjoy a lifestyle based on drugs. Because drugs are expensive, hackers need to make a great deal of money to support their lifestyle (Nicholson, Hansard 1990a: 1154).

The problems with legislation

The criminal law has no business here. For the network has no borders, and the autonomous space of hyperperfect illusion and flawlessly recombinant culture is too slippery for any statute. (Karnow 1994:8)

In one … lament, Business Week claimed that even if information thieves are caught 'it is not always easy to prosecute them. Larceny means depriving someone of their possessions permanently. Can a
person be tried for stealing a copy of information when the supposedly stolen information remains in the computer?' Similarly, Mano complained, that one 'might as well play billiards with a sash weight' as try to control computer abuse by applying existing laws to this new threat. (Michalowski and Pfuhl 1990: 268).

Peculiar status of info

you can steal a document in a company, photocopy it and take it home, and they could do nothing, maybe within the company, but there would be no criminal offence, within the company they could fire you. And then if you do the same thing with a computer it should be a criminal offence, why? In all the rest of the justice system it depends on what you do with them [documents or whatever], it depends on your intentions, and as soon as you use a computer, your intentions are no longer important, it's just that you use a computer, it's a magic area that we don't understand and that we can't control so that we must take you one step before you do harm and we must not care about your intentions: it's bullshit! (Gongrijp: Amsterdam interview).

Peculiar status of info

Mr Cohen MP warned that with the criminalisation of such activities such as non-malicious browsing: "The Bill's net is being cast far too wide, and it will lead to many people, some vulnerable, committing a crime where none now exists ... In years to come, the Bill could apply to a washing machine, controlled by a chip ... That is nonsense" (Hansard 1990a: 1166+7). Another MP asked the rhetorical question: "Are we really saying that members of staff who make unauthorised use of a firm's personal computer to produce their own CV or every perpetrator of a childish prank that their misdemeanour is worthy of a criminal record they will keep for the rest of their life?" (Leigh, Hansard 1990a: 1173).

Pace of Change

The problem is that it was six weeks ago when I first defined the word 'computer' to my satisfaction. That definition is already out of date. The passage of time and the pace of development within the computer industry mean that any definition of a computer or a computer system would soon be out of date (Hansard 1990a: 1159).