PROLOGUE

# What Makes Hackers Tick? a.k.a. Linus's Law

LINUS TORVALDS

I first met with Pekka and Manuel at an event that the University of California at Berkeley had put together in the Bay Area, a half-day symposium on the challenges of the network society. Here were these social-science big shots talking about modern technology and society. And there I was, representing the technical side.

Now, I'm not an easily intimidated person, but this wasn't exactly the kind of setting in which I was most comfortable. How would my opinions fit in with those of a bunch of sociologists talking about technology? But hey, I thought, if they have sociologists talking about technology, they might as well have a technologist talking about sociology. At worst, they'd never invite me back. What did I have to lose?

I always end up doing my talks the day before, and once

again, there I was feverishly trying to get an "angle" for the next day. Once you have that angle—your platform—writing a few slides is usually not that hard. I just needed an idea.

I ended up setting out to explain what makes hackers tick and why Linux, the small operating system that I started, seems to appeal so strongly to hackers and their values. In fact, I ended up reckoning, not just with hackers, but with our highest motives in general. I called my notion (in my normal humble and self-deprecating way) "Linus's Law."

## Linus's Law

Linus's Law says that all of our motivations fall into three basic categories. More important, progress is about going through those very same things as "phases" in a process of evolution, a matter of passing from one category to the next. The categories, in order, are "survival," "social life," and "entertainment."

The first phase, survival, is a truism. Any living thing needs to survive as its first order of business.

But the other two? Assuming you agree with *survival* as being a fairly fundamental motivational force, the others follow from the question "What are people ready to die for?" I'd say that anything for which you might forfeit your life has to be a fairly fundamental motivation.

You can argue about my choices, but I think they work.

You can certainly find instances of people and other living creatures who value their *social ties* more than they do their lives. In literature, *Romeo and Juliet* is the classic example, of course, but you can also think about the notion of "dying for your family/country/religion" as a way of explaining the notion of social ties as potentially more important than life itself.

Entertainment may sound like a strange choice, but I mean by *entertainment* more than just playing games on your Nintendo. It's chess. It's painting. It's the mental gymnastics involved in trying to explain the universe. Einstein wasn't motivated by survival when he was thinking about physics. Nor was it probably very social. It was entertainment to him. Entertainment is something intrinsically interesting and challenging.

And the quest for entertainment is certainly a strong urge. You might not feel the urge to die for your Nintendo, but think of the expression "dying of boredom": some people, certainly, would rather die than be bored forever, which is why you find people jumping out of perfectly good airplanes—just for the thrill of it, to keep boredom at bay.

What about money as a motivation? Money is certainly useful, but most people would agree that money per se is not what ultimately motivates people. Money is motivational for what it brings—it's the ultimate bartering tool for the things we *really* care about.

One thing to note about money is that it's usually easy

to buy survival, but it is much harder to buy social ties and entertainment. Especially Entertainment with a capital *E*—the kind that gives your life meaning. One should not dismiss the social impact of having money, whether you buy something or not. Money remains a powerful thing, but still it is just a proxy for other more fundamental motivating factors.

Linus's Law per se is not so much concerned with the fact that these three things motivate people but more with the fact that our progress is a matter of going through the full phase change from "survival" to "social life" to "entertainment."

Sex? Sure. It obviously started out as survival, and it still is. No question about that. But in the most highly developed animals, it's progressed past being a thing of pure survival—sex has become part of the social fabric. And for human beings, the pinnacle of sex is entertainment.

Eating and drinking? Check. War? Check. Maybe war is not quite there yet, but CNN is doing its best to get it to that final stage. It certainly started out as survival, has progressed to a means of maintaining social order, and is inexorably on its way to becoming entertainment.

## Hackers

All this definitely applies to hackers. To hackers, survival is not the main thing. They'll survive quite well on Twinkies and Jolt Cola. Seriously, by the time you have a

computer on your desk, it's not likely that your first worry is how to get the next meal or keep a roof over your head. Survival is still there as a motivational factor, but it's not really an everyday concern to the exclusion of other motivations anymore.

A "hacker" is a person who has gone past using his computer for survival ("I bring home the bread by programming") to the next two stages. He (or, in theory but all too seldom in practice, she) uses the computer for his social ties—e-mail and the Net are great ways to have a community. But to the hacker a computer is also entertainment. Not the games, not the pretty pictures on the Net. The computer itself is entertainment.

That is how something like Linux comes about. You don't worry about making that much money. The reason that Linux hackers do something is that they find it to be very interesting, and they like to share this interesting thing with others. Suddenly, you get both entertainment from the fact that you are doing something interesting, and you also get the social part. This is how you have this fundamental Linux networking effect where you have a lot of hackers working together because they enjoy what they do.

Hackers believe that there is no higher stage of motivation than that. And *that* belief has a powerful effect in realms far beyond that of Linux, as Pekka will demonstrate.

CHAPTER 5

# From Netiquette to a Nethic

## Netiquette and Nethic

Beyond the hacker work and money ethic is the significant third level of the hacker ethic that can be called the *nethic* or network ethic. This expression refers to the hackers' relationship to our network society's networks in a wider sense than the more familiar term *netiquette* (which concerns behavioral principles for communication on the Net—e.g., "avoid flaming," "read the file of frequently asked questions before posting your message," etc.).[1] Again, not all hackers share all the elements of the nethic, but still these elements are linked together in their social meaning and relation to the hacker ethic.

The first part of the hacker nethic consists of the hackers' relation to media networks such as the Net. Although we can say that hackers' characteristic relation to them dates back to the origin of the hacker ethic in the sixties,

this nethic has received a more conscious formulation in recent years. One key moment came in 1990 when hackers Mitch Kapor and John Perry Barlow started the Electronic Frontier Foundation in San Francisco to promote the fundamental rights of cyberspace.[2] Barlow, a child of the sixties counterculture, used to write songs for the Grateful Dead and became a pioneer in the cyber-rights movement. He was the first to apply William Gibson's term *cyberspace* (from his novel *Neuromancer*) to all electronic networks.[3] Kapor was an important player in the development of personal computers, creating, in 1982, the spreadsheet program Lotus. It was the first PC application that made a widespread function significantly easier than it had been before, and this made it an important factor in the breakthrough of the personal computer.[4] The name *Lotus* reflected Kapor's background: as a former mental-health counselor with a psychology degree, and later a transcendental-meditation instructor, he was interested in Eastern thought systems.

The enterprise, also called Lotus, that Kapor had built around his program quickly evolved into the largest software company of its time. But as his original hackerism became more and more entrepreneurial, Kapor began to feel alienated, and he left the business after four years. In his own words: "It felt awful to me, personally. So I left. I just walked away one day. . . . The things that were important to the business as an organism were things that I could demonstrate less and less enthusiasm for."[5]

Both Barlow and Kapor considered the fundamental rights of cyberspace, such as freedom of speech and privacy, critical issues. The immediate impetus for the Electronic Frontier Foundation was the FBI's suspicion that both Barlow and Kapor were in the possession of stolen source code. So, in popular usage, they were suspected of being "hackers" (that is, crackers), and FBI agents paid visits to both of them. The suspicion was unfounded, but Barlow and Kapor felt that lawmakers and law enforcers did not really understand what genuine hackerism and cyberspace were all about. For example, the agent visiting Barlow hardly knew anything about computers and referred to Nu Prometheus, the cracker group that had stolen the code, as New Prosthesis.

Barlow and Kapor could have shrugged off those visits, but they became concerned that a lack of understanding might ultimately lead to a totalitarian-style regulation of electronic space that could seriously weaken the freedom of speech and privacy dear to hackers. Ironically, Barlow's FBI visitor—a defender of capitalist law and order—happened to be a namesake of the Protestant preacher Richard Baxter that Weber saw as the purest representative of the Protestant ethic, almost as if the meeting had been scripted as an allegorical confrontation between the Protestant ethic and the hacker ethic.

The EFF's cofounders included Wozniak, John Gilmore, and Stewart Brand. Gilmore is known for supporting the use of strong-encryption technologies to protect pri-

vacy, and for his slogan "the Net treats censorship as damage and routes around it," in accordance with which he cofounded the Net's totally uncontrolled alt- newsgroups. Brand was the creator of *The Whole Earth Catalog* and played a significant role in the history of hackerism by writing the first article about it (in *Rolling Stone* in 1972) and by organizing the first Hacker Conference (in San Francisco in 1984).

The EFF defines itself as "a non-profit, non-partisan organization working in the public interest to protect fundamental civil liberties, including privacy and freedom of expression, in the arena of computers and the Internet."[6] In practice, the EFF has contributed to the overturning of, among other measures, the Communication Decency Act passed by the United States Congress in 1997, which tried to create a kind of censorship authority for the Internet. The EFF has also played an important part in defending the use of strong-encryption technologies previously declared illegal in the United States. Before this law was changed, the EFF, through Gilmore, constructed the DES Cracker, which was capable of breaking through the so-called DES protection used in the encryption of some bank transactions and e-mail delivery on the Net; the point was to demonstrate that the encryption methods permitted by the United States are not able to protect privacy.[7] Socially conscious hackers emphasize that encryption technology must not only meet the encryption needs of governments and businesses but

also protect the individual from governments and businesses.

Freedom of expression and privacy have been important hacker ideals, and the Net developed in accordance with them. The need for hacker organizations such as the EFF arose when, in the nineties, governments and enterprises became interested in the Net on a large scale and have since often tried to develop it in a direction opposed to hacker ideals.

In its defense of freedom of expression and privacy, the hacker world is typically decentralized. In addition to the EFF, there is a great number of other hacker groups engaged in similar activity. Two examples of these are Holland's ethically engaged XS4ALL Internet service and Witness, which reports on crimes against humanity using the tools of cyberspace. These hacker groups join forces in thematic clusters such as the Global Internet Liberty Campaign.[8]

## Freedom of Speech: The Case of Kosovo

There is more than enough for all of them to do. In the so-called developed countries, where freedom of expression and privacy are considered fundamental rights, there are nevertheless continued attempts to curtail these rights in cyberspace.[9] In the rest of the world, however, these rights are not even recognized in any clear fashion. According to *Censor Dot Gov: The Internet and Press Freedom 2000,* a

study published by the research center Freedom House, about two thirds of the world's countries and four fifths of the world's population do not have complete freedom of speech as of the beginning of 2000.[10]

When so minded, the powers that be are able to control the media, especially the traditional, centralized ones such as the press, radio, and television. They do, of course, also try to gain control over Net content, but in practice this is remarkably difficult, due to the Net's decentralized structure. For this reason, the Net has become an important medium for free individual expression in totalitarian societies. And hackers, who created this medium, from e-mail and newsgroups to chat and the Web, have helped dissidents in various parts of the world in its use.

The Kosovo crisis of 1999 is an excellent example of these attempts, seen in many other countries too.[11] Censorship is often an early-warning symptom of other forthcoming violations of human rights, and once these violations are being carried out, censorship allows for only a sanitized official version of events and prevents the dissemination of any criticism. This was the case in Yugoslavia, where President Slobodan Milosevic gradually tightened his stranglehold on the media while the country's Serb majority speeded up "ethnic cleansing" in the province of Kosovo, the Albanian majority of which wanted self-government.

Things get ugly when freedom of speech is curtailed.

While Serb forces in Kosovo executed men, raped women, and drove entire villages—from newborn children to the aged—into exile, the official media of Yugoslavia proclaimed that everything was just fine. (This tradition was continued until the last moments of Milosevic's power: after he had tampered with election results and while hundreds of thousands of people were protesting in the center of Belgrade, Serbian TV showed Olympics replays and classical music.) The media could not report on atrocities, and opponents' voices were silenced. During the NATO air strikes aimed at putting an end to the massacres, the traditional Yugoslavian media were practically taken over by the government. The academy was also silenced because it is the traditional proponent of free speech.[12] The words of Basil's rule, "No one is to . . . make curious inquiries about what is being done," described the government's policy.

The Net, however, was able to spread the news. On the initiative of the EFF, a network server named anonymizer.com provided Kosovars with the opportunity to send out messages in a way that prevented authorities from tracking them down.[13] However, the best-known messages from the war were transmitted as straightforward e-mail. A famous instance was the e-mail correspondence between "Adona," a sixteen-year-old ethnic Albanian girl, and Finnegan Hamill, a junior at Berkeley High School in California. (Adona's real identity was not revealed for security reasons.) Adona wrote:

> Hello Finnegan. . . . One night, last week I think, we were all surrounded by police and armed forces, and if it wasn't for the OSCE observers, God knows how many victims there would be. And my flat was surrounded too. I cannot describe you the fear. . . . The next day, a few meters from my flat, they killed this Albanian journalist, Enver Maloku. Someday before there was a bomb explosion in the center of town where young people usually go out.[14]

On another day she wrote:

> I don't even know how many people get killed anymore. You just see them in the memoriam pages of newspapers. I really don't want to end up raped, with no parts of the body like the massacred ones. I wish nobody in the world, in the whole universe would have to go through what we are. You don't know how lucky you are to have a normal life. We all want to be free and living like you do, having our rights and not be pushed and pushed. Finnegan, I'm telling you how I feel about this war and my friends feel the same.

Just before the beginning of the NATO air strikes, Adona sent this message:

> Dear Finnie,
> At the moment I am writing to you, just from my balcony. I can see people running with suitcases and I can hear some gunshots. A village just a few meters from my home is all surrounded. I have prepared my

> bag with necessary things: clothes, documents, and money . . . in case of emergency. Only the past few days, there have been so many new forces, tanks, and soldiers coming inside Kosovo. Yesterday, a part of my town was surrounded and there were shootings happening. . . . I am waiting with no patience for the news.

The control exercised by the Milosevic government was based both on the strict "public information law" of 1998, which permitted the closing down of the media on the whim of the authorities, and on sheer brute force. For example, in March 1999, Serb police shot and killed Bajram Kelmendi, a human-rights advocate, and his two sons. Kelmendi had been defending the Albanian-language newspaper the police had closed down. Slavko Curuvija, publisher of two independent newspapers and a man who according to government television supported the NATO air strikes, was shot down in front of his home on April 11, 1999. Dozens of other journalists were arrested, brutalized, or sent into exile.[15]

Yugoslavia's most influential oppositional medium, the radio station B92, has had continuous and varied problems with the authorities. On November 27, 1996, during antigovernment demonstrations, its transmission signal was jammed, and on December 3 it was shut down completely. At this point, XS4ALL offered to help B92 by relaying its transmissions over the Net (the sound-transmission technology was provided by RealAudio from RealNetworks, which is financed by Kapor). The Voice of

America, among others, then transmitted the signal received through the Net back to Yugoslavia. Its censorship having proved ineffective, the government soon allowed B92 to resume normal radio transmissions.[16]

XS4ALL's ideology is expressed in its name: Net access should be available to all, as the Net is a medium for freedom of expression. XS4ALL says it is ready to be "active in politics and is not frightened of lawsuits."[17] Cooperation between XS4ALL and B92 resumed at the beginning of the Kosovo war on March 24, 1999, when Yugoslavia's telecommunications ministry once again closed down the station and confiscated its transmitters. The station's editor in chief, Veran Matic, was arrested, though released the same day, with no explanation given. On April 2, the station's director, Sasa Mirkovic, was fired, and the authorities appointed a new director and prescribed new guidelines. With the help of XS4ALL, the original editors of B92 managed to continue their transmissions, again via the Net, and radio stations abroad once more transmitted the signal back to Yugoslavia.[18]

B92's victory over government control was particularly important in that the station became a symbol for independent critical media in Yugoslavia. The defense of free media written by Matic at the beginning of the war expresses well what was at stake: "As a representative of the free media, I am only too aware of the need for information, whatever side you are on in the conflict. People inside the country should be kept up to date with inter-

national debate as well as with what is happening at home. Those abroad ought to be told the truth about what is going on here. But instead of detailed, uncensored facts, all we hear is war propaganda, including western rhetoric."

Toward the end of the war, the Witness organization trained four Kosovars to document human-rights abuses on digital video. The visual material was then transmitted out of the country by means of a laptop computer and satellite phone via the Net. This material has been made available to the International War Crimes Tribunal.[19]

Witness, founded in 1992, believes in the power of images in the reporting of human-rights violations and defines its task as the development of video technology and training in its use for this purpose: "Our goal is to equip human rights defenders with the tools they need to record, transmit, and publicize human rights abuses that might otherwise go unnoticed and unpunished." Its founder, musician and cyberart pioneer Peter Gabriel puts it: "Truth knows no borders. Information wants to be free. Technology is the key."[20]

In addition to these hacker groups, even the more traditional action groups moved into "Net time" during the Kosovo conflict. OneWorld, which coordinates civilian organizations, and its partner Out There News created a Net database of refugees, to help people find their relatives and friends.[21] Even in the peace-treaty negotiations, which were naturally determined above all by human and

not technological factors, the new technology played a symbolic part. In the negotiations chaired by Finland's president Martti Ahtisaari and Russia's former prime minister Viktor Chernomyrdin, the first draft treaty was written on a Net mobile phone, and the first preliminary reports on the negotiations were sent to representatives of different countries as text messages.[22] Thus, it may be justified to call the Kosovo war the first Net war, the way the Vietnam War has been labeled the first television war.

A small part of the war was even conducted over the Net. Crackers supporting different sides launched their own attacks, as described in Dorothy E. Denning's study *Activism, Hacktivism, and Cyberterrorism* (2000). Serbian crackers disrupted the NATO server only a couple of days after the war began. A Californian cracker countered with an attack on the Yugoslav government's webpages. Crackers took sides according to their views of the conflict: the Russians and the Chinese attacked the United States, and Americans, Albanians, and western Europeans attacked Serb pages. Some eastern European crackers also created viruses with anti-NATO messages. After the end of the war, some media even spread the (false) rumor that President Clinton had approved of a plan to use crackers for operations such as the raiding of Milosevic's bank accounts.[23]

It must be admitted that the Net had only minor influence on general views of the war, and even less on its conduct. Nevertheless, there is no reason to consider it, as a

medium for free speech, as something separate from other media, since all media are interconnected in their spheres of influence. As a reception channel, the Net still is not a mass medium, but that statement demands two important qualifications. First, in some circumstances the Net may be irreplaceable as a reception channel. Via it, messages from the traditional media may reach audiences that have been prevented from receiving them by censorship exercised by their own governments. This is how many people in totalitarian countries receive information and views that are not allowed by their governments.

Second, the Net does not necessarily have to be a mass medium reception channel to have an influence on a wide public. It can be an effective production tool in the creation of reports that can then be disseminated through the traditional media. We must remember that the Net provides everyone with the tools of a journalist. Even the reporters and editors employed by the traditional media increasingly write, record video for, and transmit their stories using these tools. When computers, telecommunications, and the traditional media combine forces in one fast multimedia Net, and when the computer, the telephone, and the camera are fused into a small multimedia gadget, individuals become able to transmit reports designed for the great media machinery. Such a user of future Net appliances may not operate on a technical and journalistic level comparable to that of professionals, but these shortcomings are outweighed by his or her being on the spot

and experiencing events firsthand. In Kosovo, we have seen only the beginning of what media hackerism may achieve.

## Privacy or Electronic Omniscience

The Net may be a medium of free speech, but it can also be turned into a medium of surveillance. Traditionally, many hackers have worked to prevent this by also defending privacy in cyberspace. Recently, governments and business have tried to make inroads on this privacy in many ways.[24]

In a number of countries, there have been discussions about a so-called back door to the Net, which governments could use for surveillance when they consider it necessary, or even automatically to keep a permanent eye on people's e-mail and Web-browsing patterns. (Automated surveillance is based on programs that analyze the contents of messages and Web visits and report "dubious" cases to a human surveillance agent.) In this respect, the difference between so-called developed and developing countries seems to be that there still is a debate about these tactics in the developed countries, while in the developing countries governments already use such devices without any preliminary discussions. Thus, in Saudi Arabia Internet-service providers are obliged to keep a log of users' activity on the Web and to send an automated warning to users as soon as they try to access banned sites or pages, to remind them that they are, indeed, being watched.[25]

In developed countries, at least in peacetime, business is a greater menace to privacy than the government tends to be. Although business enterprises cannot access Internet-service providers' databases in the manner that governments can, they are able to deduce similar information in other ways. While moving around the Web, a user's browser program and webpage servers exchange information that identifies the user (so-called cookies). By itself, this does not enable anyone to know the user's personal data, but it does allow them to note each time a user $x$ visits a particular webpage. After this, the identification of $x$ can be made, at least in principle, as soon as the person gives out personal information to any website that collects such information and sells it to others. After that, $x$ has a name, a sex, an age, an address, an e-mail address, and so on. And after that, it can be known who visits dog pages, pages concerning a certain pop artist, pornographic pages, et cetera, on the basis of which a person's interests can be analyzed.

Some enterprises have specialized in the collection of such information by placing advertisements on a huge number of webpages. Since these advertisements are not really part of the page but are provided by the advertiser's Web server, the advertiser is also able to exchange identifying information with the user's browser. The main purpose of these advertisements—or, more accurately, "spy links"—is to gather information on the browsing patterns of individuals. The lifestyles of individuals are the stock in trade of these enterprises. The comprehensiveness of

the lifestyle maps they generate from this information depends on how many spy pages the enterprise is able to maintain and how much information on their visitors or clients businesses outside of its spy ring are willing to sell to them.

Messages sent to newsgroups are another essential source of lifestyle information. They are easier to analyze, since basically all messages sent to newsgroups are saved permanently somewhere, open for anyone to read. Surprising amounts of information can be gathered by simply observing what groups individuals have participated in and by analyzing the language of their messages.

In the electronic era, users constantly leave electronic traces in various databases. The more electronic our era becomes, the more traces there are to be found. Thus, as computers, telephones, and the media converge, even the television programs people watch, the radio stations they tune in to in their cars, and the articles they read in the online newspapers can be recorded in electronic databases. Through the base stations mobile-phone owners use, even their locations can be determined with extreme accuracy. With this kind of information, a very intimate image of an individual can be created.

As the number of electronic traces increases, the image of the individual becomes more and more accurate. Even today, every bank and credit-card transaction is recorded in the card company's database; if a person uses a courtesy card, transactions made with it are also recorded in

that company's database. The electronic currency of the future (whether it will be used via the computer, the mobile phone, the television set, or some other appliance) will preserve this information even more comprehensively. In the most detailed case, some database might list each and every product bought by individuals during their lifetimes. It is easy to see how a detailed profile of a person could thus be created.

Specific knowledge of an individual's lifestyle interests business enterprises for two main reasons. First, such knowledge facilitates very precisely aimed marketing: for example, when a person is known to have a dog, she or he will receive commercials for dog products on her or his digital TV during commercial breaks. (Had this person also once sent an e-mail message with the title "Cats suck," he or she would also not receive commercials for cat products.) Or if it is known that a person has a sweet tooth, she or he could receive, at appropriate moments during the day, mobile-phone messages about candy offerings at a nearby store.

Second, such detailed profiling makes it possible to scrutinize the lifestyles of workers and job applicants. The storage of people's doings in electronic memory means, ultimately, that no act remains unknown. In the electronic age, the corporate monastery's gate is guarded by a computerized Saint Peter, who differs from omniscient God only in that he is not forgiving. During the job interview, the applicant's entire life up to that moment flashes by,

and he or she has to account for all sins: at age six, you flamed your buddy on the Net in a politically incorrect manner; at fourteen, you visited pornographic websites; at eighteen, you confessed to a chat room that you had experimented with drugs. . . .

An increasing number of businesses also exercise (sometimes unannounced) surveillance over their employees' electronic behavior. Many enterprises have installed computer programs that observe employees' use of e-mail and the Web: does the employee use inappropriate language (e.g., expressions of anger); with whom is he or she in touch (not the competitor, we hope); does he or she visit sites of ill repute (those pornography pages)? Even the content of telephone conversations can be controlled in a similar manner using speech-to-text technology.[26]

Hackers have long emphasized that the maintenance of privacy is by no means a given in the electronic age but requires more conscious protection than ever before. They have spent much time discussing the pressures on privacy now exercised by businesses and governments. For the sake of privacy, some hackers have even resorted, symbolically, to preelectronic solutions in some particularly intrusive circumstances. Eric Raymond, for instance, does not use a bank card, because he is opposed to the way in which the technical operation of that system records every monetary transaction. Technically, it would have been possible to create a model in which the individual's transactions would not transmit any personal in-

formation and the business would still be able to charge the correct card. This is a matter of choice.

Many hackers abhor any violation of the individual's personal boundaries, no matter whether this takes place during working hours or outside of them. An employment relationship gives no one the right to intrude into personal territory. Danny Hillis's Zen-like anecdote about personality testing exemplifies the way hackers feel about employers' eagerness to analyze the individual ever more precisely, using all kinds of techniques: "A disciple of another sect once came to Drescher [a researcher at Minsky's AI Lab] as he was eating his morning meal. 'I would like to give you this personality test,' said the outsider, 'because I want you to be happy.' Drescher took the paper that was offered him and put it into the toaster, saying: 'I wish the toaster to be happy, too.' "[27]

In order to protect electronic privacy, many hackers have defended the use of the kinds of strong-encryption technology of which governments disapprove, since strong encryption is needed to guarantee genuine privacy. The U.S. law on arms exports formerly classified these technologies (which use a key larger than 64 bits) as munitions, and thus their sales came under strict regulation. To parody this law, one hacker tattooed on his left arm the so-called RSA encryption method, classified as strong encryption, in just three short lines of code, which he accompanied, in compliance with U.S. law, with this statement: WARNING: THIS MAN IS CLASSIFIED AS A MUNITION.

FEDERAL LAW PROHIBITS TRANSFER OF THIS MAN TO FOREIGNERS.[28]

Hacker groups played an important role in bringing about some loosening of these legal restrictions in early 2000.[29] One of the most important groups developing strong-encryption methods is Cypherpunks, founded by John Gilmore, Tim May, and Eric Hughes. Its goals are summed up in Hughes's "A Cypherpunk's Manifesto" of 1993:

> We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.
>
> We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.[30]

In his manifesto "Privacy, Technology, and the Open Society" (1991), John Gilmore fantasizes further about what a society constructed on hacker principles might be like:

> What if we could build a society where the information was never collected? Where you could pay to rent a video without leaving a credit card number or a bank number? Where you could prove you're certified to drive without ever giving your name? Where you could send and receive messages without revealing your physical location, like an electronic post office box?
>
> That's the kind of society I want to build.[31]

Hackers work to find technical solutions that will enable the electronic age to respect privacy. The Cypherpunks are by no means alone in realizing this ambition. The first functional anonymous server that enabled people to send e-mail or messages to newsgroups without revealing their identities (known as a remailer) was created by a Finnish hacker, Johan Helsingius. A member of Finland's Swedish-speaking minority himself, he describes the need for such a server: "Where you're dealing with minorities—racial, political, sexual, whatever—you always find cases in which people belonging to a minority would like to discuss things that are important to them without having to identify who they are." In another context, he adds: "These remailers have made it possible for people to discuss very sensitive matters, such as domestic violence, school bullying or human rights issues anonymously and confidentially on the Internet."[32]

In the future, privacy won't be merely an ethical question but a technological one as well. The technical reali-

zation of electronic networks has a great impact on the individual's right to privacy. The hacker nethic's defense of privacy becomes a hard cooperative effort: besides securing the Net, influence has to be exerted on a great number of other networks that store details of individuals' lives.

## Virtual Reality

Historically, the Net as a hacker medium has an important third dimension that is not often linked to the idea of the hacker ethic, although it is clearly related to the above two attitudes toward the media: in addition to the ideas of freedom of expression and privacy, hackers value the individual's own activity. In fact, *activity* is a word that sums up well the linking idea behind all three elements of the hackers' nethic. Freedom of expression is a means toward being a publicly active member of society, receiving and articulating various views. Privacy secures one's activity in creating a personal lifestyle, because surveillance is used in order to persuade people to live in certain ways or to deny legitimacy to lifestyles that deviate from the ruling norms. Self-activity emphasizes the realization of a person's passion instead of encouraging a person to be just a passive receiver in life.

In this last respect, the nature of traditional media (especially television), which makes the user merely a receiver, is very different. It takes the monastic idea of a one-way "sky channel" to its secularized logical conclusion. As early as the 1980s, the French sociologist-

philosopher Jean Baudrillard pointed out that the television viewer's symbolic apotheosis as a receiver arrived when TV shows introduced canned laughter. He noted that television had reached a point at which the TV show itself was both the performer and its own audience, "leaving the viewer with nothing but pure amazement."[33]

Even though the Net is sometimes also referred to as "virtual reality," nowadays the television viewer just as frequently experiences his situation as virtual, in the sense of *unreal*. As it stands now, watching television characteristically elicits a feeling that what is being seen must be meant as some kind of absurd parody of what television could be at its worst.

The experience of unreality is enhanced by the glaringly obvious way in which television has become part of the economy. Increasingly, television companies operate on the same pure profit-motive basis as any other business. The essential thing for them is the viewer ratings, because they enable them to sell commercials. Programs have fundamentally become advertisements for the commercials, and viewers are needed only to raise the price of time. An important motivation for traditional media to expand operations onto the Net is the fact that these new technologies offer the chance to gather very detailed information on users, which thus enables the sale of even more precisely targeted advertising. The goal here is to use technology to enhance market-driven audience segmentation.

Since television is connected so closely to capitalism, it

is also, in large part, dominated by the Protestant ethic. This connection illuminates the previously discussed threats to freedom of expression and privacy by contextualizing them as yet another confrontation between the Protestant and the hacker ethic. The commercial character of the media both prevents any focus on commercially uninteresting regions or subjects and leads to violations of privacy.

But one can also argue that if our lives were not so determined by the Protestant work ethic, people would not put up with the current offerings of television. Only when work uses up all energy and people are too tired to enjoy the pursuit of their passions are they ready to be reduced to the passively receptive state suited for television.

The rise of the network society does not in itself give any reason to believe in the general illusion, promulgated in books such as Jeremy Rifkin's *The End of Work*, that the role of work would be automatically diminishing in our life and that our energy thus would be freed for more leisurely pursuits. In fact, in the last couple of decades actual work time has not become shorter but has actually become longer. Any claim of a reduction in working hours can be justified only by a comparison with nineteenth-century industrial society's most extreme twelve-hour workday, but not when it is seen in a more general historical or cultural context.

Furthermore, the mere duration of work time does not provide a comprehensive point of comparison. We must

remember that any abbreviation of work time has always been made at the cost of optimizing the remaining work time even further. Shorter working hours do not by any means imply that people are working less. On the contrary: even though working hours have grown shorter than they were in the industrial society's worst-case scenario, they have been optimized to be even more demanding on a person than before. Shorter working hours do not mean a diminution of work or work-centeredness if the same (or even greater) results must be achieved in less time.

In his book *Closing the Iron Cage: The Scientific Management of Work and Leisure*, sociologist Ed Andrew analyzes how the nature of work guided by the Protestant ethic returns us easily to a passive lifestyle in yet another way: "It is not that sociologists of leisure are wrong to think that many workers are incapable of expansive enjoyment off work but rather that they do not take sufficiently seriously the view that incapacity for leisure is a 'spillover effect' of externally managed work."[34] When the individual at work is still treated as a dependent receiver, a trend is encouraged in which leisure is also reduced to passive amusement, with no room for active passions. According to Andrew, only when an active work model has been achieved will active leisure also be realized: only when individuals become self-directed in their work will they be able to become active creators in their leisure time.

The lack of passion in leisure time is truly doubly tragic

when it results from a lack of passion during working hours. In this case, the Friday-centeredness of life is realized in the most absurd way: managed in their work externally, people wait for Friday in order to have more time to watch television and be externally amused. Hackers, on the other hand, use their leisure—Sunday—as an opportunity to realize personal passions other than those that they pursue in their work.