Joseph ‘Jofish’ Kaye

STS.532: Inside Technology

Due 17th December 2003

Completed 6th February 2004

Hacking: An underrepresented practice in STS

Abstract

Hacking is an attitude and practice surrounding the use, consumption, and production of computer-related work. I propose that the study of hacking behaviors is an intriguing alternative to the institution-based work in science and technology that dominates STS discourse. In this paper, I show how characteristics of hacking are found in a multitude of domains, starting with canonical computer hackers at MIT 1965-1985, and show similarities to rural car users at the beginning of the century and radio hams 1900-1975. I conclude that the key features of hacking are that it happens in a social context, that it has an irreverent attitude to the technology, that it is concerned with hands-on ways of knowing and learning and that is generally performed by males.

Introduction

As I hope to show, the ethos behind hacking has a long legacy, dating back at least to the beginning of the century. Nowadays, the hacker is presented by the media as a powerful outlaw figure, breaking into computers, stealing credit card numbers and other personal information, and pirating software, music, and video. This is not the kind of hacker I propose exploring: rather, I am investigating a practice of irreverent use of technology, breaking apart traditional producer/ consumer boundaries. This notion of hacking has a long tradition of use. (Leibowitz 1990; Raymond 1996; Peterson 2002) In the last ten or twenty years, however, 'hacking' has been used and arguably hyped by the media (Skibell 2002) to mean the practice of breaking into computer systems to change things, to steal for personal gain, or just for destruction.   I'm going to follow the lead of the hacking (in the first sense) community and refer to such malicious hacking as 'cracking' (Raymond 1996), and the phenomenon under study as hacking. The practice is similar to the practice Haring (2002) refers to as 'tinkering'; I'll discuss my reasons for my choice of vocabulary at later point.

Our mental picture of a hacker is an unwashed, unshaven young man leaning over a keyboard in the early hours of the morning, fueled by high-caffeine soft drinks, coffee, and vending machine food. In this paper, I will propose that this is not the be-all and end-all of hackerdom, and that hacking is an important phenomena that occurs in many technological domains. In particular, I will attempt to characterize salient characteristics of hacking, and show how they occur in other domains.

I. Computer Hacking

The canonical example of the hacker is indeed the computer hacker, as exemplified in Steven Levy's hagiography of the development of computing, *Hackers*. (Levy 2001) He discusses of four groups of hackers: the group centered around MIT's Tech Model Railroad Club and later the AI Lab in the fifties and sixties, the development of Silicon Valley in the seventies, the growth of the game company Sierra Online in the eighties, and finally devotes an epilogue to Richard Stallman prior to his leaving MIT to devote himself to free software. Other works exploring this history include (Sterling 1992; Freiburger and Swaine 1999)

Of these, the first section tells stories of late night programming sessions stretching the limits of human endurance. A typical story is the conversion of an assembler written for the TX-0, an earlier machine, to the PDP-1, a newer machine:

> Kotok, Samson, Saunders, Wagner and a couple of others began on a Friday night late in September... They wouldn't change inputs or outputs and wouldn't redesign algorithms... And they wouldn't sleep. Six hackers worked around two hundred and fifty man-hours that weekend, writing code, debugging, and washing down take-out Chinese food with massive quantities of Coca-Cola... It was a programming orgy, and when Jack Dennis came in that Monday he was astonished to find an assembler loaded into the PDP-1... (Levy 2001)

This is as we've been led to expect from hackers: unwashed, unshaved young men working in the wee hours of the morning. A little deeper reading reveals some interesting insights, however.

The first observation that is that that unshaven young man is not working in isolation. The chapter abounds with various organizations: The Tech Model Railroad Club, and particularly the Signals and Power Subcommittee – the group in charge of the vast array of electronic equipment that controlled the large model railroad at the center of the club's spiritual and physical space – are key players. Faculty members at MIT, notably John McCarthy and Marvin Minsky appear, but only as far as they give their groups of students an identity and auspices under which to use the computers. These groups had varying degrees of formality and informality, but functioned together, with knowledge and skills transferring between them, through casual interactions, through newsletters, and through looking over each others' shoulders. As computing grew, the role-call of groups, both formal and informal increased: the growth the AI Lab and their rival Lab for Computer Science, DARPA and the relationships between local communities it engendered, and above all the hackers and their informal associations.

This notion of informality and corresponding irreverence is interesting and problematic. The hackers Levy describe have no truck with bureaucratic nonsense designed, as far as they're concerned, to keep them away from the computers they want to spend time on. There is little patience with officially endorsed priesthoods whose job it is to limit access, or who put artificial limitations on what can and cannot be done with the machine. This is not a manifestation of a generalized lack of respect – hackers were respectful and generally pleasant to each other, if frequently socially inept – but an attitude towards authority, and, more importantly, an attitude towards the machines themselves.

However, at the same time, the behavior occurs within highly structured institutions: the computers themselves were paid for by MIT, by DARPA, by the Labs as separate organizations. There's a continual tension between the anti-organization rhetoric of the hackers and the pressures of the institutions that contain them. This tension and back-and-forth seems to be a characteristic of hacking communities: some might argue that it's characteristic of any individuals working in institutions, but the emphasis on individual relationships and individual respect for each other brings the contrast to the foreground.

This notion of respect for each other is key. It is related to hackers' notions of status, which is earned through action and implementation. There is perhaps a begrudging respect for theorists, but the emphasis is on execution of the hands-on. Previous work is relevant and can bring status and respect, but the application to the job at hand is what's key: if that knowledge cannot solve the current problem, the one at hand right now, it is not important.

This notion of the world as a series of problems to be solved is fundamental to the idea of hacking. It ties into a lack of respect for authority. The causes for said lack of respect are two fold. First, if status within in the community is a function of hands-on execution, then authority figures have no innate status. There is no barrier to attaining this status – Levy cites Minsky as being an authority figure respected by the hacking community for his hacking skills – but there is an assumption that respect must be gained. The second cause for lack of respect for authority is the emphasis on problem solving. The trappings, the paraphernalia, the tools that make authority function are seen not as legitimate boundaries, but as more problems to get around and to solve when necessary. Rules are not broken for the sake of breaking them, but when they become obstacles to the solving of a larger problem.

This problem solving, and the lack of respect for barriers to said problem solving, motivates the activity of hacking itself. It's an act of breaking open black boxes, understanding the content and disseminating that knowledge – partly to solve the immediate problem at hand, but also with the recognition that breaking open the box and understanding the contents will be useful at some later stage to either the hacker himself or to another hacker at a later date. This information is disseminated back into the hacker community, leading to recognition of the knowledge acquired by the hacker and a corresponding rise in status.

An interesting reflection of this attitude is shown in a time-sharing system known as ITS, implemented on the then-new and powerful PDP-6. ITS implemented a number of novel functions, of which perhaps the most interesting was KILL SYSTEM. Levy explains:

> Formerly, a hacker rite of passage would be breaking into a time-sharing system and causing such digital mayhem – maybe by overwhelming the registers with looping calculations – that the system would "crash". Go completely dead. After a while, a hacker would grow out of that

> destructive mode, but it happened often enough to be a considerable problem for people who had to work on the system. The more safeguards the system had against this, the bigger the challenge would be for some random hacker to bring the thing to its knees before it bombed....
>
> ITS, by comparison, had a command whose specific function was crashing the system. All you had to do was type KILL SYSTEM, and the PDP-6 would grind to a halt. The idea was to take all the fun away from crashing the system by making it trivial to do that. (125)[1]

It's possible that this attitude towards problem-solving that also is related to a notable characteristic of hacking communities: they're mainly male.[2] There's a great deal of work on the male dominance of computing and hacking communities: (Olerup, Schneider et al. 1985; Hacker, Smith et al. 1990; Rasmussen and Håpnes 1991; Spertus 1991; Berner 1997; Faulkner 2000; Klief and Faulkner 2002) just to begin with. There are female hackers, and very good ones indeed, but a study of the motivations behind their scarcity can wait for a

[1] A similar decision was made with MIT's campus-wide computing system, Athena, where the root password to all workstations is public knowledge. "Hacking root", or trying to get the top-level control of a computer, has a long history, and the cry of success, "Woot!" has become integrated into other online cultures outside of hands-on hacking. But this is a more complicated issue than I want to go into, and has a lot to do with the design of a network of public-access workstations.

[2] Pop psychology books (I'm thinking of Men are from Mars, Women are from Venus) tell us that men treat situations as problems to be solved, whereas women treat the situation as a state: when men discuss problems, they only feel better when there is a solution, whereas women gain catharsis and the ability to deal by the act of discussion.

later paper. For now, we'll just recognize this as a characteristic of hacking without deeply understanding it.

These characteristics seem to be key ones expressed around the community of computer hackers under discussion. In summary, they are:

i. Hacking occurs in a social context
ii. Hacking is irreverent and informal, and this is in tension with the various institutions that support hacking
iii. Respect is gained through hands-on problem-solving
iv. Hacking is concerned with opening black boxes and understanding their content.
v. Hackers are mainly male

I feel there are two more points that need to be made to complete an accurate picture of hacking. The first characteristic concerns the motivation of hackers. The key understanding, which underlines the reconsideration that the notion of hacking brings to traditional models of supply and demand, is that hackers don't hack for profit: they hack for fun. There are hackers who find a way to profit from their hobby but the primary motivation is to learn and explore for the sheer joy of it.

There is more extensive work around this problem: in the social sciences, Kleif & Faulkner's excellent (2002) article, *Boys & Their Toys*, discusses issues socialization and legitimacy as motivators around "men's love affair with technology," but conclude that much the work done by males around technology is done for the pleasure of so doing.   A different approach to the same question is taken by Shah and her colleagues at the MIT Sloan School: relying on extensive questionnaires and interviews with open-source programmers, they came to the conclusion that most of their subjects do what they do for two reasons: because they have a problem to solve, and because they enjoy programming. So:

vi. Hackers hack for fun

It is interesting to compare these hackers with another class of users that has been extensively documented: the lead user. 'Lead user' is a term invented by Eric von Hippel at the MIT Sloan School to describe extreme users of a particular product: those users who are pushing the item to its limits, modifying it to meet their particular needs. von Hippel advocates that companies look to lead users as a source of innovation and new product concepts. (Hippel, 1988; Shah, 2000) Perhaps the simplest explanation is that the hacker who has realized that they can make money from their hobby is an entrepreneur; the lead user is a hacker who someone else has figured out they can make a profit from.

The final point is so obvious as to almost escape notice: hacking is performed upon technology. Levy's discussion, and the discussions around gender and computing, above, imply that hacking is uniquely performed on computers. As a primary point of this piece, I propose relaxing this definition and including other aspects of computing; I hope to show that the tight fit of our other definitions justifies such a move. Thus:

vii. Hackers work on technology

We now have seven characteristics of hacking: it is social, irreverent, respects hands-on learning, is concerned with opening black boxes, and is mainly done by males, on technology, for fun[3]. I now go back to that last point, in which we widened our definition of hacking from computers to technology, and look at some other documented domains to see if our characteristics fit observed behaviors.

[3] In Levy's book, he lists seven elements of the "Hackers Ethic". These correspond in some part to our characteristics of hacking, and are worth mentioning here, although I do not feel they are as useful to us as this list. They are:

- "Access to computers – and anything which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative!
- All information should be free.
- Mistrust Authority – Promote Decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer
- Computers can change your life for the better"

II. Rural Automobile Users, 1900-1930

Pinch & Kline's article (Kline and Pinch 1996) and later book (Kline 2000) explores the practice and rhetoric around the use of cars as engines to power equipment on farms, from pumping water and grinding corn to sawing wood and running the washing machine. This practice has similarities to computer hacking, but also some interesting differences.

i. Social Aspects: The Grange, the *Rural New Yorker*, and Communities

An initial reading gives the impression that the various communities around these approaches to automobile use were more organized than the computer hacking communities we saw in part I. There is more emphasis on letters to and articles in newspapers and journals –the *Rural New Yorker, Motor Age,* the *Ford Times.* But it's hard to determine how much of this is a result of the historical nature of the study. The vast majority of Levy's work was done through interviews with the leading characters in the story, many of whom were not just still alive but still involved in some aspect of hacking computers.

Kline's work emphasizes the textual source by necessity, and it's hard to separate method from content here. There is some information in that many of the letters quoted are from sources like 'one Kansas farmer, George Schmidt' in the *Rural New Yorker,* from 'T.A. Pottinger of Illinois' in *Wallace's Farmer,* 'one rancher', 'a Tennessee farmer', 'a Maine farmer'. (Kline 2000 66-68) These are not professional mechanics: they are amateurs participating in a social change of information, through their role as a farmer, or, alternately, through their role as a motorist, in magazines such as *Motor World*. Although it was clearly a social undertaking, there is insufficient evidence in the article and the book chapter to characterize this statement much further.

ii & iv. Irreverence & Opening the Black Box

Where this case study seems to show the simplest parallels to hacking is in their treatment of the technology regardless of the intended uses of the manufacturer. Kline & Pinch go into some detail about the varied reactions of four groups they identify as responding to the reshaping of the automobile on the farm: automobile manufacturers, farm equipment manufacturers, gasoline-engine firms and newly-emergent accessory companies. It is clear, as a first step, that in general the automobile manufacturers were not enthusiastic about their clients opening up the black box of the automobile.

> ...[C]ompanies...usually discouraged using the car as a stationary power source by jacking up its rear wheels. In response to a survey on this question by the *Rural New Yorker* in 1906, six out of seven auto manufacturers adamantly opposed this common practice[4], mainly because it could damage the engine or differential gear...
>
> Based on these responses, the *Rural New Yorker* advised farmers over the next decade to purchase a stationary gasoline engine...instead of using the

[4] The article goes on to state that the Ford Motor Company was more forgiving of such uses, at least up until the time they developed their own purpose-built tractors designed for modification.

> car as a stationary power source, even though several technically competent farmers wrote that they had had good luck with the practice. (Kline & Pinch 1996 784)

This last line is intriguing: it demonstrates both a degree of irreverence for the corporate advice on behalf of the farmers, but also points to the tension played out in the journal's pages between the intended audience and the (advertising-providing) automobile manufacturers. Neither chapter nor article gives the impression of the nose-thumbing attitude to authority seen in the case of our computer hackers, but it's clear that corporate tut-tutting was seen as no barrier to the creative use of the vehicle to solve problems on the farm.

iii. Respect for each other

Neither article nor chapter gives any background on relations between farmers as individuals regarding mutual respect. It seems unlikely that this was not the case, but there is not exploration thereof in the texts.

v. Gendering the automobile

There is an interesting division in Kline (2000) and in Kline & Pinch (1996) between the gendering of the use of the automobile as a car, and the gendering of the use of the automobile for other tasks – the practice we have identified as hacking. The automobile as a car was open to gendered interpretation: "Male and female access to the drivers seat varied widely across families", "some women drove the car to the exclusion of men"; "at least [sic; not 'only', surprisingly] two of the twenty-three familes interviewed recently in New York said that a mother or daughter did not learn to drive.” (779)

However, the same cannot be said of the reinterpreted automobile. Pinch & Kline state:

> Our evidence overwhelmingly shows that farm men, not farm women, reconfigured the car in order to use it in an alternative manner. We have found only one exception – that of an independent woman farmer who used her car to pull a hay rake in 1918.

This gendering of the ‘hacked’ automobile as opposed to the automobile-as-car seems significant. Perhaps even more so than in the field of computers (Spertus 1991), we see a gender division between legitimized and alternative uses of the technology.

vi. Automobile as technology

No surprises here: the automobile is fundamentally approached as an item of technology – culturally embedded and becoming more so, but clearly technological.

vii. For the fun of it: the pleasure of hacking

This is perhaps the most significant difference between the hackers we see at MIT in Building 26 and in the AI Lab, and the farmers we see on their farms. The hackers are doing what they do pretty much just for the sheer joy of so doing. Sure, they’re working on projects, but in general, we’re seeing as much effort put into writing a compiler as writing an adventure game: it’s for the joy of the game as much as anything. These professional farmers are in a different situation: their reconstitution of the automobile is directly and tightly tied to their professional work and income. They may be using techniques similar to those of the hackers, but they're doing it with a clear eye on their profit margins.

It seems, therefore, that while these farmers may have used methodologies that look extremely similar to those of computer hackers, their motivations were significantly different. I now propose looking at a different section of culture: that of radio amateurs.

III. Radio Amateurs, 1900-1980

Kristen Haring's doctoral thesis, *Technical Identity in the Age of Electronics* (Haring 2002) explores the world of the American radio ham in the 20th century. These radio hams share many of the characteristics of computer hackers: an emphasis on the role of hands-on learning, tight social networks, an emphasis on the free dissemination of information, crossover between work and play, and a love of the beauty and elegance of the machine.

Haring does not use the word 'hacker'; she uses the term 'tinkerers': a group that seem to have many of the same characteristics as hackers. However, I feel that the term tinkerers implies a lack of technical ability, someone messing in something they shouldn't, a casual attitude to perhaps fixing or mending slightly broken things. 'Hackers' implies, I hope, a deeper relationship to technology, a hands-on immersion that I feel is both more accurate and perhaps more respectful to the subjects in question.

For our purposes, the hams and the hackers have one very significant difference: to become a ham, there is a formal process of certification, administered by the FCC. Haring describes these structures as being part of the definition of the community, enforced by the community themselves:

> "Through enculturation and policing – a process of teaching, expectation, criticism, punishment, and, in extreme cases, expulsion – the community enforced the boundary and behavior rules it established." (74)

This process of certification, dating from 1912, marks a strong difference between the computer hackers and the radio hackers. There are no certifications for entry in the computer hacking community; Levy's Hacker Ethic states that *Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position*, and to a large extent this remains the case. At the same time, however, the ham community negotiates issues of informal social networks and hierarchy around the formal certification, and questions of theoretical vs. hands-on learning and teaching. Ham radio represents a rich source of discussion around such issues.

i. Social: QSL Cards & Clubs

At a fundamental level, the ham radio process is a social undertaking. The fundamental ritual of ham radio is to establish a contact with someone, ideally someone a long way away, and then confirm that contact by postcards, known as QSL cards. As such, it is inherently a social undertaking, although it appears perhaps strangely structured from the outside.. However, there are also social structures closer to home.

One effect of the certification process is to provides a focus for organized groups of hams, engaged in teaching the next generation the skills and knowledge they'll need to pass the FCC certification exam, and, simultaneously, ensuring the survival of the . These same communities also served as forums for discussions and exchanges of advice, ranging from informal discussions or hands on demonstrations to mimeographed club newsletters, to glossy ham magazines. (204)

However, once these minimum levels of certification are achieved, Haring shows evidence of rich social networks. There are newsletters, face-to-face meetings, and extensive traffic in postcards sent from one ham to another as physical evidence of their meetings on air. Furthermore, the certifications, particularly after the decision of the FCC to allow 'incentive certification' – certification past the basic level ham level – provide a nexus of skill transfer around which clubs would form, with mentoring relationships between individual members and the dissemination of study aids and the like.

ii. Irreverence, or, What is the greater good?

The notion of irreverence is problematic in ham radio. On one hand, there is a very hacker-like irreverence to the technology itself: Haring devotes an entire chapter to issues surrounding the controversy between building hobby equipment and purchasing off-the-shelf. She states:

> Amateurs came to see building as central to hobby identity, yet I also document their attraction to readymade gear. In every decision to buy or build, a ham faced a choice that struck at the core of his identity as an active hobbyist. (274)

Conversely, the ham community has a much less adversarial attitude to authority than the hacker community. This is in some way a function of the FCC's licensing of the field, but it runs deeper than that. Both WWI and WWII saw extensive cooperation between the ham community and the military, including the formation of the "Naval Communications Reserve" for those who could send and receive Morse code at a rate of ten words a minute. The Army developed the "Army Amateur Radio System", which organized civilian volunteers to teach soldiers about radio and leveraged amateurs' expert[5] knowledge to give advice to army engineers about equipment design. Both of these were due to the extensive training process necessary for military radio operators: Haring states that teaching nonhams to be military radio operators took three to four months; licensed amateurs took only two weeks to make the transition. (65)

Perhaps the clearest difference in attitude between hams and hackers comes in the founding statement of the Radio League of America, one of the earliest radio clubs, which included in its founding statement of purpose the promise to act "as a defense

[5] Yay! That just needed footnoting.

unit for the US in the event of hostilities, and to check on and report such activities of German agents in this country as they might have." (63) It is hard to imagine any of the organizations connected to hackers in the latter part of the century allying themselves with the government in this manner.

I think this may point to the key difference between hackers and hams. While both have similar characteristics, the former arose from a culture of modernity, of technical innovation seen as leading progress, with patriotism and technology intertwined as bastions of a growing America. Hacker culture grew in the midst and the legacy of the Vietnam war and the Sixties, with the rise of the university as center for liberal opinion, and what grew into a postmodern dismissal of technological determinism. Both, wonderfully, were young men believing strongly that what they were doing was the Right Thing to do, and happy to use their joy in technology to further their ethical underpinnings. Arguably, the attitude to technology does not change; the social milieu and corresponding manifestation of that attitude differs.

iii. The Hands-on & The Professional: Amateur Ways of Learning & Doing

Prior to WWII, the vast majority of amateur equipment was built by the ham themselves. However, with the advent of the transistor and, quickly thereafter, the integrated circuit, building one's own equipment became problematic for hackers with skills they had built up using circuits of vacuum tubes and wires. Haring quotes handbook author William Orr, writing in 1957:

> The manly art of building your own receiver is almost as extinct as the famous dodo bird... A decade ago the home-made receiver was the rule rather than the exception. (277)

The tension is evident between the desire for hands-on, hacker-type learning is at odds with the professionalization of the engineer over the 1950s and beyond, a process that encouraged book learning and theoretical understandings over hands-on doing. I believe this tension helps understand the hacker attitude to hands-on work: a similar professionalization and theoreticization of computer science and computer-related engineering happened and is happening from the fifties to the current day, and following the discussion of Haring (p274-284), I think hands-on imperative can be seen as part of a response by a community that feels it is under attack from those have emphasis on the theoretical over the practical – without such an opposition, there's no need for the added emphasis.

iv. Black boxes: opening & building

In many ways Haring's subjects do not take apart black boxes: their hobby is one of construction. Haring states:

> "Constructing equipment was so closely identified with the ham community that in 1973 the Realistic Guide to Electronic Kit Building credited radio amateurs with being "the true hobbyists who started the build-it-yourself concept in electronics." Building provided the practical training essential for technical interactivity and the chance to fully control a machine from its creation. This section traces the importance of construction in ham radio to the opportunity for learning by doing.

> Amateurs came to see building as central to hobby identity, yet I also document their attraction to readymade gear. In every decision to buy or build, a ham faced a choice that struck at the core of his identity as an active hobbyist." (274)

Having said that, the discussions Haring presents between hams concern the workings of another black box: the atmosphere. The discussions of atmospheric conditions, of sunspots, of reception seem similar to the discussions of hackers attempting to open black boxes. Hypotheses are put forward, current conditions and recent attempts and successes are discussed. Both build tools (rigs, software) to hack the black box in question; in both, the aim is not necessarily to build a tool to use to solve the same conditions, but to push the boundaries of what's possible forward each time.

v. Men & Boys

Ham radio, much as computer hacking, is primarily a male occupation. Haring describes a culture ranging from one in the manner of traditional gentlemen's clubs, with smoking and drinking a key part of meeting activities, to rowdy goings-on, notably at the annual joint meeting of the Northern and Southern Californian DX's Clubs in Fresno, complete with heavy alcohol consumption and illicit liaisons. The numbers back up this impression: founded in 1946, the Northern California DX Club went from 13 initial members to more than 150 by 1970; it was all-male until 1963 and had only three woman members by 1972. (257) This is typical of amateur radio of the time.

vi. Technology

Clearly, amateur radio work is deeply involved with hacking technology, although interestingly mitigated by the fact that the technology is a tool to hack the atmospheric conditions, as discussed above.

vii. Fun & work

Radio and computer hacking are in a similar situation with their relationship to making profit. Neither have profit-making as a primary motive, but both have complex relations between skills learnt as a hobby and at the workplace: in Haring's first chapter, she documents studies showing licensed amateurs earning, on average, twice the average wage. Both Haring and Levy do document institutions who hire those with amateur skills, including companies composed primarily of each kind of enthusiast; nevertheless, profit is not the primary motivation behind either set of hackers' actions.

III. Discussion

If we take the preceding to be examples of this phenomena of hacking, we can extract some interesting similarities and differences between them.

These case studies point to shared threads in all these instances of technology use, appropriation and development. For example, there is a problematic relationship between the institutional and the non-institutional in each case.

Radio hams are proud of their amateur status, but many work for technology companies, and their work and hobby skills build on each other. Computer hackers espouse the free flow of information and software – made possible by their employment by corporations or government-funded educational laboratories.

Key to each one of the case studies examined here is the absence of profit as an (initial, at least) motivation for the users' actions. There are cases in which users do find a way to profit from their hobbies: as in the many radio hams who Haring documents using the skills learned in their hobby at work, or the entrepreneurs Levy documents in his later chapters. However, the primary motivation is not to make money, but to learn and explore for the love of technology itself.

Communities build up in the course of each of these efforts. Status transactions occur in each community: status is gained by displaying and sharing knowledge, and such status and corresponding respect gives the hacker an opportunity to participate in the community and thus receive information that is useful to them to accomplish their personal goals with the technology.

In summary, our criteria have stood up reasonably well to inspection. Hacking is indeed a social endeavor, grounded in and creating communities around it. It is irreverent, but, and this is key, irreverent to the black box created around the technology, not necessarily to authority per sae. It has an emphasis on hands-on ways of learning and doing, but that knowledge is transferred back into the community to repay the hackers' knowledge and social debt to the group. It is primarily but not exclusively a male approach to technology.

The key understanding from this paper is the emphasis on the irreverence to technology. It is not a lack of respect for technology – far from it. It is a familiarity that leads to an understanding of what is possible with technology, and that familiarity cannot coexist with a reverent attitude.

Having said that, I feel this paper opens up far more opportunities for discussion than it answers. It brings up issues of the relationship between institutional cultures and individuals, and issues of systems and technological responses to marginalization within those systems. It raises a rich set of concerns around gender and technology. It ties tightly into current debate in S&TS about the role of skill and expertise, (Collins and Evans 2002) particularly as it applies notions of amateur ways of learning and doing to debates around tacit knowledge. (Collins 1974) It raises questions of boundaries and configuring the user (Oudshoorn and Pinch 2003): the very notion of user implies a boundary between producer and consumer that hacking culture questions. I believe that these issues make hacking culture a rich and as of yet understudied domain for science & technology studies.

References

Berner, B. (1997). Gendered practices : feminist studies of technology and society. Linkèoping, Sweden, Stockholm, Sweden, Department of Technology and Social Change Linkèoping University ; Distributed by Almqvist & Wiksell.

Collins, H. and R. Evans (2002). "The Third Wave of Science Studies: Studies of Expertise and Experience." Social Studies of Science **32**(2): 235-296.

Collins, H. M. (1974). "The TEA Set: Tacit Knowledge and Scientific Networks." Science Studies **4**: 165-185.

Faulkner, W. (2000). "Dualisms, Hierarchies and Gender in Engineering." Social Studies of Science **30**(5): 759-792(34).

Freiburger, P. and M. Swaine (1999). Fire in the Valley, McGraw-Hill.

Hacker, S., D. E. Smith, et al. (1990). Doing it the hard way : investigations of gender and technology. Boston, Unwin Hyman.

Haring, K. (2002). Technical Identity in the Age of Electronics. History of Science Department. Cambridge MA, Harvard University.

Klief, T. and W. Faulkner (2002). Boys and their Toys: Men's Pleasures in Technology. Wie natürlich ist Geschlecht? Gender und die Konstruktion von Natur und Technik. U. Pasero and A. Gottburgsen. Wiesbaden, Westdeutscher Verlag. **8**.

Kline, R. and T. Pinch (1996). "Users as Agents of Technological Change: The Social Construction of the Automobile in the Rural United States." Technology and culture **37**(4): 763 (33 pages).

Kline, R. R. (2000). Consumers in the country : technology and social change in rural America. Baltimore, Johns Hopkins University Press.

Leibowitz, B. (1990). The Journal of the Institute for Hacks, TomFoolery and Pranks at MIT. Cambridge MA, MIT Press.

Levy, S. (2001). Hackers : heroes of the computer revolution. New York, Penguin Books.

Olerup, A., L. Schneider, et al. (1985). Women, work, and computerization : opportunities and disadvantages : proceedings of the IFIP WG 9.1 First Working Conference on Women, Work, and Computerization, Riva del Sole, Tuscany, Italy, 17-21 September, 1984. Amsterdam ; New York, New York, N.Y., North-Holland ; Sole distributors for the U.S.A. and Canada Elsevier Science Pub. Co.

Oudshoorn, N. and T. Pinch, Eds. (2003). How Users Matter : The Co-Construction of Users and Technology. Cambridge MA, MIT Press.

Peterson, T. (2002). Nightwork. Cambridge MA, MIT Press.

Rasmussen, B. and T. Håpnes (1991). Excluding women from the technologies of the future? A case-study of the culture of Computer science’. Sex/Machine. Readings in culture, gender and technology. P. D. Hopkins. Bloomington & Indianapolis, Indiana University Press.

Raymond, E. S. (1996). The new hacker's dictionary. Cambridge, Mass., MIT Press.

Skibell, R. (2002). "The Myth of the Computer Hacker." Information, Communication & Society **5**(3): 336-356.

Spertus, E. (1991). Why are There so Few Female Computer Scientists? MIT Artificial Intelligence Laboratory Technical Report. Cambridge MA, MIT Artificial Intelligence Laboratory.

Sterling, B. (1992). Hacker Crackdown. Bantam.