Paper to be presented at the DRUID Summer Conference 2006 on

**KNOWLEDGE, INNOVATION AND COMPETITIVENESS:
DYNAMICS OF
FIRMS, NETWORKS, REGIONS AND INSTITUTIONS**

Copenhagen, Denmark, June 18-20, 2006

Track G: Corporate Innovation, Strategy and Organization

HARNESSING THE HACKERS: THE EMERGENCE AND EXPLOITATION OF OUTLAW INNOVATION

Stephen Flowers
Complex Product Systems Innovation Centre
Centre for Research in Innovation Management (CENTRIM)
Freeman Centre, University of Sussex
Falmer, Brighton BN1 9QE
Tel: 01273 877933
Fax: 01273 877980
Email: s.h.flowers@brighton.ac.uk

Date of submission: May 2006

Abstract

This paper will explore how the often illegal activities of hackers (in the original usage of the term to refer to individuals who modify computer hardware and software) may produce valuable innovations. It will explore how these innovations, termed Outlaw Innovations, may be appropriated by firms and provide case studies where this has taken place. The paper will seek to locate this phenomenon in the existing innovation literature, and explore the implications for firm innovation processes. It will outline a series of possible research questions and conclude by indicating the next steps in the development of this research.

keywords: innovation, users, hackers

JEL - code(s): M10, O31

1 Introduction

Good ideas are found in many places and firms will routinely draw on a range of sources, both internal and external, as part of their innovation process. Structural changes, including the growth in the number of knowledge workers, has led to innovation becoming 'democratised' (von Hippel, 2005) or 'Open' (Chesbrough, 2003). Firm innovation may now require novel and evolving relationships with a large number of external actors whose ideas may be bought, licensed, or else are freely revealed. However, in addition to these more established sources of innovative ideas firms are now seeking to exploit the innovations that emerge from the often illegal activities of a particular form of user – the hacker[1].

Although the potential for users to provide new ideas and indicate future market trends is well understood, (e.g. von Hippel, 1986, Thomke and Von Hippel, 2002), often implicit in this established view is the existence of a cooperative and consensual relationship from which both user and supplier will seek to benefit, facilitating a free flow of information between the two parties. But this is not the only kind of relationship that may exist and this paper will examine innovations that arise from attempts to: amend a product's functionality or in some other way extend or distort the intentions of the original designers; exploit design flaws in order to attack or evade security systems; or create systems or services in order to compete with mainstream commercial firms.

These activities may violate intellectual property and pose a direct threat to established suppliers with the result that the work will often be underground in nature, operating either anonymously or with those involved seeking to obscure their links to such activities. Within this milieu, innovations will emerge from non-cooperative, non-consensual relationships in which the user may be unknown to the supplier and in which there is likely to be no free flow of information between the two parties.

This paper will propose that such activity, at least within IT-intensive digital industries, is widespread and often operates in parallel with mainstream use in this area. It will argue that such outlaw innovations may be adapted by firms and supplement mainstream innovation processes, directly impacting on firm R&D, and potentially leading to new improved products and new markets. The paper will introduce the notions of Outlaw Innovation and Outlaw User, locate these concepts in the innovation literature, provide examples of this phenomenon, and explore the implications for firm innovation processes. The approaches that firms employ in response to such activity in order to either resist or appropriate the innovations that Outlaw Users generate will be outlined, and the paper will explore how the challenge presented by Outlaw Innovation can act to supplement in-house innovative activities.

The paper is structured as follows: section 2 will explore how the role of the user is explored within the innovation literature and introduce the concepts of outlaw innovation and the outlaw user; section 3 will introduce a provisional typology of outlaw users; section 4 will present a series of case studies that examine individual outlaw innovations and explore firm reactions to such activity; section 5 presents a discussion and explores implications for our understanding of the role of the user in innovation; section 6 will present brief conclusions and outline a series of questions to guide further work in this area.

2 Innovation and the User

Innovation is a cluster of processes that takes new ideas and moves them into widespread application. It will typically involve design, manufacturing and marketing of a new (or improved) product (Freeman, 1982), that may be either a radical or incremental improvement on the state of the art (Gardiner and

[1] It should be noted that the use of the term 'hacker' is not applied in the prejorative sense, but rather to refer to individuals who create and modify computer hardware and software.

Rothwell, 1985). In the case of industrial innovation, such activities have traditionally taken place within firms which often have large internal R&D facilities organised around such work (e.g. Xerox Parc, Bell Labs, the Thomas J. Watson Research Laboratory at IBM). It has been argued that this approach, now known as closed innovation, no longer reflects the way in which firms will utilise ideas sourced externally and that may have originated in other firms. This view, termed open innovation (Chesbrough, 2003), is a recognition that firms may no longer rely on their own R&D efforts and may buy or license ideas from other companies. In this context the boundary between the firm and other external actors becomes far less distinct than in the closed innovation model, with firms able to draw on a variety of external sources of R&D as part of their innovation strategy. Although such external sources are generally understood to include such things as firms, universities and joint ventures, this paper will explore how firms seek to exploit ideas obtained from Outlaw Innovation.

Within this discussion a key distinction exists between invention, the development of a good idea, and the process of bringing that idea into widespread use, innovation. This has sometimes been referred to as the process of commercialisation (Teece, 1986), although this view is limited as it ignores a wide range of innovative activity that is non-commercial in nature, but which bring new ideas into wider use (e.g. public sector innovation, open source innovation). It is argued that Outlaw Innovation is another such non-commercial activity that falls outside this narrow definition but, as we shall see, is a potent means by which novel ideas are brought into widespread application.

2.2 The User

The term ‘user’ can be problematic as its meaning largely depends on context and the tradition of the literature within which it is employed. For example, within the innovation literature the term ‘user’ generally takes an upstream, supplier-centric, perspective and in this context the ‘user’ (e.g. lead user, final user, user innovation, learning by using) tends to be at the level of the firm. As a result the user tends to be examined as an adjunct to supply-side issues like product development and market demand. For example, users have been characterised as consumers whose needs must be understood for a product to stand any chance of being a commercial success (e.g. Rothwell, Freeman et al 1974). It has also been recognised that the expertise and experience of certain kinds of user may be harvested and applied within a supplier’s product development activities. For example, tough customers (Gardiner and Rothwell, 1985) who make exacting demands may have a positive benefit on innovation by driving suppliers to further develop products, thereby widening their potential market. In contrast lead users, (von Hippel, 1986) may modify or develop existing products in response to their exacting and non-standard needs, often foreshadowing future market demand. The involvement of (firm-level) users in firms’ product development processes by developing and distributing supplier-designed ‘toolkits’, enabling users to engage in innovation by developing their own custom products (von Hippel and Katz, 2002; Thomke & von Hippel, 2002) has been explored, although their role in influencing the direction of user innovation is less clear.

It has also been argued that the process of innovation is becoming democraticized as improvements in ICT enable users to develop their own products and services, freely sharing their innovations and creating a rich intellectual commons (von Hippel, 2005). That users will often freely share their innovations with others, termed free revealing, has been widely documented (e.g. Franke and Shah, 2003; Nuvolari, 2004) and this forms a key element in the rapid dissemination of innovations and in their adoption by manufacturers.

These conceptions of user-supplier innovation all tend to depict a relationship in which the supplier is able, in some way or another, to harness the experience or ideas of users and apply them to their own product development efforts. The potential for users, either as individuals or as groups, to become involved in the design and production of products has been recognised for some time. The term ‘prosumer’ was coined (Toffler, 1980) to describe professional consumers who, no longer content to be a passive market for suppliers, would become actively involved in product design. This conception, in

some ways foreshadowing the idea of the lead user, does however continue to locate the process of production with the supplier. However, the boundary between production and use has blurred, particularly in information rich digital environments like software, publishing, music and design. In this context some users are able to develop and extend technologies and the distinction between user and producer, or 'users' and 'doers' as Castells would have it (Castells, 1996), essentially disappears. The emergence of this behaviour has led to what has been termed a democratising of innovation (von Hippel, 2005) that is particularly apparent in these digital environments.

The activities of users in the co-development of computer games is an example of this blurring of use and production that has led to new and different types of relationship between users and producers (Jeppesen et al, 2003) and has led to firms exploiting the unpaid work of enthusiastic users (Postigo, 2003; Kuchlich, 2005). As we have seen the (largely consensual) appropriation of user ideas and experience is a recurrent theme within the innovation literature. The relationship between user and manufacturer is very different where users are actively seeking to develop new ways to hack, crack, or modify products, or where they are creating entirely user-developed products that are intended to compete with mainstream firms. Although such relationships are likely to be very difficult, if they exist at all, the potential advantages (and challenges) of gaining access to this group of users has been recognised (Mollick. 2005), although there are few insights as to how this may be achieved.

3 The Outlaw User

The emergence of the Outlaw User is likely to bear a direct relationship to the growth in the number of highly technically skilled individuals, variously termed 'intellect workers' (Baran, 1961), 'knowledge workers' (Drucker, 1959; Chesbrough, 2003) or 'elites' (Mollick, 2005), that exist within the economy as a whole. It has also been noted that one implication of this growth in knowledge workers is a shift in the structure of firm-level innovation processes (Chesbrough, 2003). However, although these elites may form the primary motor of Outlaw Innovation, the systems products and ideas that they develop are adopted by a much larger group of individuals who simply *use* these outlaw innovations. As a group, Outlaw Users are thus a combination of elite users and the much larger group of users who demonstrate their willingness to adopt these outlaw innovations.
For the purposes of this paper Outlaw Users are defined as individual users who actively oppose or ignore the limitations imposed on them by proposed or established technical standards, products, systems or legal frameworks. Outlaw Users may create or use novel hardware or software modifications to existing products, or exploit security loopholes to gain unauthorised access to systems. They may invent and bring into widespread use novel software or other systems that facilitate the sharing of digital content and enable illegal music sharing, or develop software to 'enhance' computer games. By definition, Outlaw Users will generate Outlaw Innovations, here defined as novel hardware or software modifications to existing products, systems that exploit security loopholes to gain unauthorised access to computer and other systems and protocols, algorithms and other systems that facilitate the illegal sharing of digital content. The Outlaw User operates within a technology-rich environment and, as a group, have produced conceptual and technological innovations, many of which have been adopted in some form by mainstream firms.

The Outlaw User is broadly hostile to the supplier's constraints on the approved methods of product use, or the laws that circumscribe its use, and may wish to undermine, avoid, or bypass them, or even adapt products or systems for their own ends. In this sense the Outlaw User may possess similar characteristics to that of a lead user (e.g. technical prowess, a need that potentially foreshadows future demand) and may even be part of the same group. One difference between the two groups is that the Outlaw User will often actively seek anonymity from the manufacturer of the product or system they wish to hack. This may be because their actions violate a product's warranty, misuse a supplier's IP, or are illegal – perhaps all three. Thus, in a very real sense Outlaw Users may be viewed as the outlaws of innovation and whilst

lead users may be sought out by manufacturers for largely positive reasons, Outlaw Users may be tracked for entirely negative reasons and, as a result, may go to elaborate ends to avoid detection.

The activities of any group of Outlaw Users will often cluster around a particular product, technology, or some other shared goal. The internet is likely to provide the primary means for communication within and between these groups and be their main means of dissemination. The activities of the technical elites and their supporters (e.g. filesharing, hacking products and systems) may be of dubious legality or else be clearly illegal. As a result the elites and their supporters are likely to be at risk of legal action and may thus operate anonymously, under a pseudonym or take other measures to evade detection by the authorities.

3.1 Outlaw Users: a typology

This section will introduce an exploratory typology of Outlaw Users, focusing on three broad classes of such activity. This typology is not intended to be comprehensive, but is merely illustrative of the types of Outlaw User activities that exist.. It should be also recognised that the exemplars used to illustrate the concept come from information-rich digital environments and it is unclear how broadly the concept can be applied to other industries or sectors.

Product Hacker. Tinkering with products to alter their performance characteristics has a long established tradition. For example, within the custom modding[2] scene for cars many aspects of appearance and performance are routinely modified, including engine modifications for use in street racing, trick suspension, sound systems, etc. Tinkering with software and computers to alter how they work has also been around for some time, with an early example being the upgrading of system clocks in IBM PCs in order to make them operate at a higher speed, and thereby enable the user to obtain better performance. This hardware modification (which involved simply removing the existing system clock and replacing it with a faster one sourced from a third-party supplier) was relatively straightforward. However, as we have seen, the level of technological capability that now resides within the user population is now far higher and a subset of users are now able to reverse-engineer, clone, re-program, and restructure many complex high-technology products.

The presence of such technically able individuals within their user community presents a potential challenge to manufacturers who are now less able to exercise control over the way in which products are used. Such elite users may no longer accept the product or system ‘as-is’, but will attempt to do things with it that the manufacturer had not intended and does not want them to do. The existence of this activity, and firms opposition to it, has been crystallised by the enactment of the Digital Millennium Copyright Act (DMCA) in the USA explicitly prohibits this activity and makes it an offence to tamper with digital copyright protection systems (Tang, 2005).

A Product Hacker is a user who will seek, in some form, to change hardware or software products by either using or developing specialised modifications. In order to develop such modifications product hackers will often reverse-engineer existing products or systems, potentially violating the manufacturer’s IP or violating other copy-protection laws in the process. The intent of product hackers is broadly to test or alter the performance boundaries of the product or system, potentially in directions that the manufacturer wishes to avoid. This is distinct from beta-testing, a practice in which firms make available a pre-production version of a product to users and request feedback concerning bugs or their problems that are detected.

[2] Modding is a term used to describe the modification of a product to perform a function not intended or authorised by the manufacturers. In the context of digital technology, modding may be used to refer to changes to hardware or software.

File Sharer. The sharing of digital content (e.g. music, video, etc) over the internet, termed file sharing, is a large and growing activity that has emerged and has been readily adopted by mainstream firms and users. Although the scale of illegal music downloading continues to be significant - although hard to estimate, it involves something like 6 million users and 800 million files at any one time (CRIA, 2005) - legal sales are also large, with the market leader iTunes alone selling more than 1 billion downloads (Apple, 2006) between April 2003 and February 2006. The File Sharer is a user who shares digital content or produces systems or software that facilitates such activity. The activities of file sharers includes the development of software designed to dismantle systems designed to protect the IP of the copyright owners of digital content by preventing illegal copying, and the copying of the digital content itself. It also includes the development of the protocols designed to enable the distribution of digital content over the internet or across local area networks, and the creation of internet sites (e.g. Napster) designed to facilitate such sharing. Finally, it also includes the individuals who upload or download digital content.

Black Hat. A Black Hat is an individual, sometime referred to as a cracker, who subverts computer security without authorisation usually by taking control of a remote computer through a network. Such individuals may penetrate computer security systems for many reasons including curiosity or as a demonstration of their technical prowess, but also vandalism, fraud, theft, and other forms of crime. Black Hat cracking routinely employs such techniques as the Trojan Horse, Social engineering and Root Kit software. A Trojan horse is a program that appear to be one thing, whilst actually being something else surreptitiously. In the context of computer security a Trojan horse is an application that fools a user into using or downloading it, thereby compromising their computer's security. Social engineering refers to the use of techniques to manipulate users to either provide information or agree to download software without their informed consent. A Root Kit is a software toolkit employed by hackers for concealing the fact that a computer's security has been compromised.

4 Exploiting Outlaw Innovation

This section will provide examples of the scope and scale of Outlaw Innovation and explore how firms have attempted to exploit this activity. It will present three exemplar cases of Outlaw Innovation relating to the typology outlined above. The cases show how firm reactions to outlaw innovation will differ and may be modified as firms learn how to appropriate the output of such activity within their own innovation processes. Additional examples are also summarised in table 1. The cases are presented as an exploratory study designed to examine key issues and research questions (Yin, 1989) that are intended to form part of a future programme of research. As such, the cases are not presented in order to build theory (Eisenhardt, 1989) but to provide a counterpoint to existing accounts of user-supplier interaction within the innovation studies literature, and in this sense aims to provide an account against which researchers can compare their experiences and gain theoretical insights (Dyer, Wilkins, 1991).

4.1 Computer game Modding

This case charts the emergence of the computer games industry from 1960's hacker culture and explores how firms moved from a tolerance of user hacking activities to their encouragement and the eventual absorption of such activities within the business model of some firms.

The computer game industry is a huge and rapidly growing market that is predicted to be worth over $21bn globally by 2007 (ELSPA, 2005) and is increasingly linked with other media like films. From its beginning as Spacewar, a two-dimensional spaceship shoot-em-up game created in 1962 on a PDP 1 minicomputer by a group of MIT hackers (Levy, 1984; Markoff, 2005), this industry now produces games designed for consoles (e.g. Sony PlayStation, Microsoft Xbox), PCs, hand-held consoles (e.g. Nintendo DS, Sony PSP), mobile phones, and mobile music players (e.g. Apple iPod). Originally

designed for single players, computer games have evolved to include single, multi-user and massively multi-user game environments in which thousands of users can play on-line simultaneously.

Computer games development has its roots in hacking culture and there is a long history of developers inserting hidden features in commercial games, sometimes termed Easter Eggs (Takahashi, 2005b). Modern games for platforms like PS2 also include features that can only be unlocked using obscure 'cheat codes' that give gamers access to additional levels, challenges or other aspects of the game. On PC-based games this 'insider' feel is far stronger and gamers now often have the facility to develop their own modifications (or 'mods') to many aspects of a game. The creation of such mods (often termed modding) by users has become a significant source of innovation within the gaming community, and firms have reoriented the way in which they develop and publish games in order to harness this source of innovation. The scale of such activity is huge, with one internet site devoted to modding noting that it has over 1.2 m unique visitors each month viewing 200,000 page views on average each day (Moddb, 2006).

However, modding was not always so popular with users nor such an important part of the business model of some games developers, but emerged out of what has been described as the 'hacker ethic' (Levy, 1984), something that is at the core of product hacking. One of the earliest recorded mods in 1972, Adventure, was a variation on a text-based computer game that gave rise to a craze of similar game mods based around Dungeons and Dragons or Star Trek (Kushner, 2002). With the development of personal computers like the Apple II and IBM PC modding moved out of the computer science labs and by the early 1980's mods appeared for commercial products like the WWII shoot-em-up game Castle Wolfenstein (Au, 2002), and arcade games like Pac-Man (Kushner, 2002).

Modding continued to develop and by the 1990s enthusiasts were able to create entire levels for games like Duke Nukem, but were also creating development designed tools to improve the mod production process. Although this activity clearly violated aspects of the game developers IP, the industry had grown in parallel with such outlaw activity and modding was viewed as an aspect of the industry's relationship with its users. A key stage in the development of this relationship came in 1993 with the release of Doom, a science-fiction horror game, that was the first product of its kind intentionally designed to make it easier to develop mods (Kushner, 2002). This was achieved by developing a software architecture that made it less likely that users would damage the game and, ultimately, by releasing the entire source code. This led to the creation of a large number of mods, which in turn helped sales of the game and by the middle of the 1990s many PC-based games were released with software that enabled users to create their own mods, some of which were radical departures from the original game.

This relationship between game developer and the modder community developed further as individual ideas or even entire versions of games developed by modders were adopted by firms. Individual modders were also finding employment within the games development industry on the back of their modding work. Although the boundary between industry and modder appeared to be becoming increasingly blurred, outlaw activities had become absorbed and now formed an important part of one part of the industry's business model. An example of this integration can be found with the game Counter-Strike.

Counter-Strike is a multi-user on-line counter-terrorism game that has been recognised as one of the most popular games of its type (GameSpy, 2004). The game was originally developed in 1999 as a mod to the game Half-Life, which itself was a full mod of Quake (Kucklich, 2005). Counter-Strike was developed by a small group of modders and was later acquired by the developer of Half-Life, Valve Software (who also employed the lead modder). Valve Software also moved to further include modders within its business model by creating an on-line distribution network for mods (the Steam system) which includes licensing and payment mechanisms for modders who wish to release their games.

Although the once outlaw activities of product hackers or modders have been absorbed into one part of the computer games industry, their activities are less welcome in other parts of the industry that will take strong action to stop such activities. Mods or product hacks of consoles are routinely met with legal

action and firms will often seek to discourage or distance themselves from game mods. For example, game publishers and developers sought to quash a mod (called Nude Raider) of the PC game based on Lara Croft, and the Hot Coffee feature locked in Grand Theft Auto: San Andreas (which, when unlocked, contained scenes of a sexual nature) led to the game being re-rated ‘adults only’ with significant controversy developing over game content and the role of games in the moral corruption of youth (e.g. McCullagh, 2005). A similar backlash has affected a mod to the Sims 2 game that displays the characters naked (Takahshi, 2005a).

4.2 Adware and Spyware

This case examines two instances of the way in which firms utilised a series of techniques often associated with Black Hat hacking. Anti-spyware legislation was introduced in 2005 by many States in the U.S. and following legal action both firms, Sony BMG and InterMix, were forced to withdraw products that included either adware or spyware.

The emergence of Black Hat hacking or cracking and its threat to computer systems has been well-documented (e.g. Stoll, 1989). Individual crackers (e.g. Dark Avenger, Captain Crunch, Jaeger, Electron, Zero-G) and groups (e.g. Chaos Computer Club, Cult of the Dead Cow, Legion of Doom, Masters of Deception) have emerged as a significant threat to computer users. Crackers continue to be arrested and computer viruses and worms continue to be released on the internet and a computer security industry has grown up to cater for government, commercial and domestic computer users. This section will explore the link between the techniques traditionally employed by Black Hats and the emergence of Spyware and Adware.

Spyware is a type of software that has been designed to intercept or take partial control of a computer without the user's informed consent. The intent of such software is generally to covertly gather information and forward it to advertisers or other interested parties. Adware is a type of software that automatically loads and displays advertisements or other marketing material when the user has not requested it.

Spyware and Adware gain access to computers through a number of routes including file downloads, web browsers, shareware or even computer viruses. Such software will often exploit security holes in web browser or other software to infect the computer. Spyware and Adware are distinct from cookies which are variables set by Web sites (including advertisers) which can be used to track Web-browsing activity, for instance to maintain a "shopping cart" for an online store or to maintain consistent user settings on a search engine. However, advertisers also often use cookies to track people's browsing among various sites carrying ads from the same firm and thus to build up a marketing profile of the person or family using the computer. It is for this reason that many users object to such cookies, and that anti-spyware programs offer to remove them. The surreptitious methods and technologies underpinning Spyware and Adware bear many similarities to the means traditionally adopted by Black hat crackers.

In November 2005 The Electronic Freedom Foundation (EFF), together with two leading law firms, filed a class action lawsuit against Sony BMG demanding that the firm repair the damage done by the software it had included on over 24m CDs. The State of Texas also sued Sony BMG under Texas Spyware legislation.

These cases arose when it emerged that Sony BMG had begun to include software on its music CDs to limit the number of times a single disc could be copied. The technologies employed, XCP and MediaMax, were termed spyware because they secretly transmitted details about what the computer is playing, and masked the files that were installed (MSN, 2005). The EFF suit alleged that the XCP and SunnComm technologies were installed on the computers of millions of unsuspecting music customers when they used their CDs on machines running the Windows operating system. It was shown that XCP had many of the qualities of a rootkit since it was designed to conceal its presence and was extremely difficult to remove. The MediaMax software, included on over 20 million CDs, had similar characteristics.

The MediaMax software was designed to install files on the user's computer even if they did not agree to the End User License Agreement and did not include a way to fully uninstall the program. In common with the XCP software, MediaMax covertly tracked users' listening habits and sent data to SunnComm through an Internet connection whenever CDs were played. This despite the fact that the the End User License Agreement stated that the software would not collect personal information (EFF, 2005). In December 2005 Sony-BMG agreed to a settlement that included an exchange scheme and compensation for those who had purchased infected CDs.

In a similar case, in April 2005 the State of New York sued the internet marketing company Intermix, alleging that the firm was the source of spyware and adware that had been secretly installed on millions of home computers. In its case The State of New York documented at least ten separate web sites from which Intermix or its agents were downloading spyware, providing either no warning or misleading disclosures. It alleged that Intermix and its agents downloaded more than 3.7 million programs to New Yorkers alone, and tens of millions more to users across the US. It was also stated that Intermix went to great lengths to protect the spyware and adware it secretly installed. The programs were hidden in unlikely locations on the computer and could not be removed through a computer's "Add/Remove" function. In addition, the programs omitted "un-install" applications, and even reinstalled themselves after being deleted. A settlement for this case in favour of the plaintiff was agreed in December 2005.

Spyware has also been associated with computer games (Ward, 2005), file sharing systems like Kazaa and even computer printers (Jett, 2004). The scale of Spyware dissemination is very significant, with a recent study finding that 80% of users in the survey had some form of spyware, with an infected computer having some 93 spyware/adware components on average and 1059 spyware/adware components found on the worst affected computer in the survey. In addition, some 89% of respondents were unaware of the spyware/adware that had been placed onto their computers (AOL/NCSA, 2004).

4.3 Filesharing

This case will provide a brief overview of the emergence and development of illegal filesharing, the introduction of legal download services and the ongoing innovation in this area.

Napster was launched in the autumn of 1999 and was the first major file-sharing service to be offered over the internet. It was the first peer-to-peer (P2P) file sharing service that enabled users to freely share music files and led to allegations by the music industry of large-scale copyright violation by its users. Although it was possible to download music before Napster was launched, the system was instrumental in redefining music consumption. It enabled users to obtain popular songs in digital format without having to purchase the single or album and also enabled users to obtain tracks already purchased on another format (e.g. vinyl), making the creation of custom compilations possible. All of this activity took place outside the normal commercial channels and Napster lacked any mechanism for collecting and distributing royalties or controlling the distribution of content. As a result, a series of lawsuits were filed against Napster, generating publicity and attracting increasing numbers of users. At it peak in February 2001 Napster had 26.4 million users worldwide (Comscore, 2001), but after a series of lawsuits and a failed appeal Napster was ordered to prevent the trading of copyrighted music on its network and was shut down in July 2001. It was subsequently re-launched as a legal service in 2003 offering a range of purchase and subscription models.

The emergence, growth and ultimate demise of Napster demonstrated three things: the existence of a large market for music file sharing; that the business model used by Napster was unsustainable; and that the technical architecture it had empoyed was vulnerable to legal attacks. This led to the launch of many more legal and illegal file sharing services and a series of innovations in file-sharing protocols (see below). For example, in April 2003 Apple Computer launched iTunes, a legal download service that was integrated with its iPod music player. The iTunes system is a digital media player application that connects to the iTunes Music Store which allows users to purchase digital music, video and audiobook

files that can be played by iTunes. Songs purchased from the iTunes Music Store are copy protected with Apple's digital rights management (DRM) system.

The integrated nature of the iTunes system has been designed to provide users with a great deal of flexibility in terms of uploading music from CD or downloading it from the iTunes Music Store, organising music into playlists, recording new CDs, and copying files to audio players like the iPod. It has also been the focal point for a number of innovations in legal downloading including the emergence and distribution of spoken audio files (podcasts – a form of asynchronous radio broadcast), music videos and other video files, and linking album art to the downloaded track. As a new entrant to the music industry, Apple's position on illegal file sharing was based on competition:

> "We're going to fight illegal downloading by competing with it. We're not going to sue it. We're not going to ignore it. We're going to compete with it." Steve Jobs[3].

Since the closure of the original Napster system and the launch of legal download services like iTunes illegal file sharing has continued to develop and unofficial Napster-style servers have proliferated using a more sophisticated generation of P2P protocols. Designed as fully decentralized networks, these have been much more challenging for copyright owners to pursue in the courts. An indication of the scale of the activity may be obtained from a recent BPI (British Phonographic Industry) report which listed the following as the 'more well-known' systems being used to fileshare illegally: Kazaa, Grokster, eDonkey, LimeWire, Morpheus, Overnet, Direct Connext, BitTorrent, Soulseek, Bearshare, iMesh, WinMX, Ares, Gnutella, Grabit (BPI, 2005).

Protocols are a key element in the development of file sharing and innovation in such protocols has come as a direct result of the challenges faced by file sharers. A major challenge took the form of the legal onslaught on the original Napster service that resulted in it being closed down. Although this version of Napster was a form of P2P service that enabled users to share files between computers connected to the network, its technical architecture was based on a series of central servers that maintained a record of the computers that were connected and the music files they contained. The presence of this central server enabled Napster to become a relatively accessible target for legal challenge and led to the development of P2P protocols that did not require such a centralised server. An example of such a protocol is embedded within the Gnutella file sharing network.

Gnutella is a P2P file sharing protocol that operates without a central server, enabling files to be shared directly between users and thereby overcoming one of the limitations of Napster. The first Gnutella client program was released in 2000 and, given the impending closure of Napster, was quickly adopted. Although the source code was later released the system was also reverse-engineered and open source versions launched. The shift of the development of the protocol into the open source community led to it being used within a large number of file sharing clients including Gnucleus, LimeWire and Morpheus. The move to open source also means that the protocol continued to evolve and an open source community emerged to support its future development. Building on the Napster experience, Gnutella is an example of a second generation protocol that is able to provide true P2P, scalability and resilience. So-called Third generation protocols are those that also build in user anonymity and encryption with the intent being to enable anonymous, censorship-resistant file sharing (e.g. GNUnet, Freenet, Entropy) although these have yet to be widely adopted.

Table 1 about here

5 Interpretation

[3] Steve Jobs, quoted in Kahney, L iTunes, now for the rest of us, Wired News, Oct 16 2003, http://www.wired.com/news/mac/0,2125,60851,00.html

Outlaw innovation is a force that has produced powerful forces for change in product architecture, business models and regulatory environments and has impacted on the nature and direction of innovation efforts deployed by mainstream firms. As we have seen, Outlaw Innovation largely operates outside or on the border to traditional regulated environments and thus is free of the restrictions that apply in those environments. It is also operates on a largely informal basis and may be driven more by challenge and curiosity than financial reward, something that it shares with free software and open source work. Outlaw innovation operates in a networked fashion via the internet and can operate in direct conflict with commercial interests. Finally, outlaw innovation may have a malicious or criminal intent, or alternatively may just be for fun, with the result that activities like modding have been referred to as 'Playbour' (Kuchlich, 2005).

5.1 Exploring the link between outlaw user and lead user

The notion of the Outlaw User is clearly related to notion of the lead user, but also differs from it in a number of important respects. Lead users are defined by the possession of two key characteristics: that they are at the leading edge of an important market trend or trends and may possess needs that will be later shared by many other users; they anticipate relatively high benefits from obtaining a solution to their needs, and so may choose to innovate (von Hippel, 2005). Applying the lead user characteristics to each of the groups in the typology of Outlaw Users reveals some interesting insights into the way in which the lead user notion sits uneasily with this form of innovative activity.

Turning to Product Hackers, the main aim of this group is to change hardware or software products by either using or developing specialised modifications. In certain cases (e.g. Sony Aibo, PC game Modders) product hackers may well be the leading edge of a market trend, but in other cases (e.g. SDMI, Sony PSP, Mac OSX for Intel, console game Modders) they may act more like a subversive group whose aim is to break the technical and legal boundaries manufacturers place on products' use. This latter group may not necessarily represent an important trend in wider demand market since their impact on the product may well be increased by the magnifying effect of the internet. This magnifying effect, enabling a relatively small number of technically gifted individuals to share their innovations within the larger group of Outlaw Users who may then deploy them, demonstrates how small groups are able to have a disproportionate impact on firms. This can also be observed in the context of another group within the typology of Outlaw users, file sharing.

Within the filesharing ecosystem digital content is decoded and is made available via sites that make use of one or more filesharing protocols, enabling files to be downloaded. At the core of this ecosystem are the technical elites who create systems to decode content, sites to publish that content and protocols that enables content to be distributed. These groups will probably exactly conform to the classic conception of lead user, as demonstrated by the very large number of individuals that make use of their innovations. The emergence and growth of a distribution system for digital content that bypasses mainstream business models and largely ignores existing IP and other laws, and is widely used by millions of Outlaw Users is an interesting example of lead user theory. It is likely that iTunes could not have launched as it did if Napster had not created the market for digital downloads of music and other content. The launch of iTunes (and the many other legal download services) thus represents an example of how both the idea and the approach of downloading that emerged as an outlaw innovation has been successfully adopted by mainstream firms.

The cases outlined provide examples of many of these facets of what is traditionally understood as user involvement in the process of innovation. For example, the SDMI case is a clear attempt to tap into the expertise and experience of a wide range non-traditional users paralleling the learning by using or trying that has been noted in more traditional user-supplier relationships (e.g. Rosenberg, 1982). The adoption of the innovations created by PC Modders also finds parallel in earlier research (Thomke and von Hippel, 2002; von Hippel, 2005). Both of these cases largely mirror traditional supplier-user relationships since

the initial 'product' has been provided to users by supplier firms who are seeking to harness user expertise in order to improve it in some way.

However, if we turn to cases in which the 'product' has been developed by (and for) outlaw users then the traditional supplier-user relationships found in the literature no longer apply. In this situation firms are faced with a parallel economy in which users design, build, develop and use products without any obvious interaction with firm-based innovation systems. The case of filesharing is perhaps the most obvious example of this activity. Filesharing is a vibrant system of innovation and use that is global in scope and continually evolving in order to react to its environment. Innovations are to be found at all levels of the system and many actors are involved in the activities of innovation and use. Much the same is likely to apply to Black Hat hackers, and although their medium of expression are the products produced by firms, Product hackers present a similar economy, albeit one that is more clearly linked with firm innovation.

5.2 Exploring the links between Outlaw and Mainstream Innovation

The linkages between the innovation regimes and outputs that outlaw users and mainstream firms inhabit will have implications, both for the appropriability of outlaw innovations and their implications for existing products, business models and regulatory regimes. The cases explored in this paper indicate that the innovations produced by outlaw users can also i) provide an important source of R&D and ii) provide a source of challenge for existing products, business models and regulatory regimes. The implications of these observations will be explored below:

Organisational responses to Outlaw Innovation
In this section the part outlaw users play in this respect is explored together with the ways in which their outlaw innovations may be appropriated by firms. The approaches that firms appear to be using in order to react, and possibly appropriate, outlaw innovations have been broadly categorised into five organsational responses.

Monitor. In this reaction to outlaw innovation firms will closely observe the activities of outlaw users in order to either react to or else appropriate what they have observed. For example, the Aibo case illustrates how, once it had retreated from litigation, Sony appears to have appropriated many of the ideas and approaches first developed by the product hacker Aibopet. Similarly, The cases of the Sony PSP and Apple OSX for Intel appear to show how these firms appropriate knowledge of the weaknesses in their products into their product development regimes reacting, in the case of Sony, by frequent updates in product firmware. Finally, the SDMI case was an example of a firm seeking to discover both the weaknesses in their product and the methods by which these weaknesses could be exploited.

Attack. Firms may choose to respond to Outlaw User activity by taking aggressive action against them, usually in the form of litigation. This was observed in many of the cases and has also been a recurrent feature associated with the emergence of illegal filesharing as a widespread activity. Firms may also seek to mould policy and concerning intellectual property, influence national legislation and strengthen copyright regimes.

Adapt In certain circumstances firms will aim to adapt or copy the technologies, methods or other innovations that have been developed by outlaw users. For example, the filesharing case demonstrates how the emergence of Napster catalysed the latent demand for being able to access music and other digital content over the internet, creating a huge market. Although iTunes is very different from Napster in that it is a pay service delivered in a traditional way (not P2P) and contains digital rights management that has limitations on use, it clearly appropriates the central idea embodied in the first outlaw version of Napster. Similarly, the emergence of the bittorrent file sharing protocol is a significant technical innovation that was developed on the fringe of outlaw innovation and, whilst it solves a major challenge associated with sharing very large files, it does not have any provision for digital rights management or a

charging regime. The announcement by Microsoft that it intends to develop a similar protocol is another example of an Adaption response by a mainstream firm. The emergence of spyware and adware is another example in which mainstream firms have attempted to adapt the ideas and methods, if not the technologies, embodied within outlaw innovations.

Influence. In this approach firms seek to influence the direction and nature of the efforts of outlaw users. This may be done by informal recognition of the efforts of outlaw users and refraining from litigation, potentially offering a tacit encouragement. Firms may go further and adopt a more open position concerning source code, may make available toolkits to enable users to engage in development, and create an 'official' web presence for disseminating those tools and for users to share their mods. This would appear to be an attempt to move previously outlaw innovation into a more ordered environment, using the development toolkits to influence the direction that outlaw innovation will take, and easing the process by which the innovations that emerge may be appropriated. This may be seen both in the Aibo case and in the example of PC game modders and represents an extension in our understanding of the way in which firms have deployed toolkits (Thomke and von Hippel, 2002).

Absorb. If an innovation is highly attractive to a mainstream firm, the skills possessed by outlaw users are rare, or the boundaries between mainstream firms and outlaw users are unclear, firms may seek to absorb both outlaw innovations and the outlaw users that understand or created them. The case of the PC game modders is a demonstration of an industry that grew out from hacker culture and was able to develop a level of intimacy with its user population that is unusually high. The tolerance and even encouragement of outlaw innovation within the industry led, in product terms, to a blurring of the boundaries between user and firm, with modders making major contributions to the level of innovation within the industry. In this context a wide range of ideas, approaches, techniques and other innovations are adopted by mainstream firms and the business model of some firms now reflect the degree of appropriation that takes place. Participation in modding, no longer necessarily an outlaw activity, is now a route into the mainstream industry, with many modders having been employed on the strength of their work. Another example of absorption may be found in the computer security industry that has grown up in response to the threat posed by Black Hats or crackers, with many 'ex' Black Hats finding employment in mainstream firms.

Firms may choose to deploy several of these approaches at the same time. For example, a firm may move to attack Outlaw Users whilst simultaneously seeking to develop other strategies that could enable the firm to adopt their innovations in some way, or influence the direction of their activities. For example, filesharing presents a highly complex scenario in which many actors are simultaneously pursuing different strategies. In this case the incumbant firms are maintaining a high level of attack on Outlaw Users, whilst seeking to develop and promote their own download services which themselves appropriate the central ideas embodied in the early outlaw filesharing innovations. At the same time a new entrant to the market, iTunes, moved directly to Adaption and has continued to innovate at a rapid pace. In contrast, whilst one section of the computer games market appears to be developing ever closer links with modders, other parts continue to keep them at arms length.

Each of these approaches are not without their own problems since the character and direction of Outlaw Innovation is, by its very nature, largely beyond the control of mainstream firms. The fundamental uncontrollability of outlaw users can lead to unpredictable outcomes. For example, although firms have managed to harness the activities of those involved in the modding of computer games, mods continue to emerge that either violate copyright, enable players in on-line multi-user games to cheat, insert inappropriate sexual content into games (e.g. the 'Hot Coffee' mod), potentially damaging the games sector as a whole. The inclusion of the SonyBMG spyware onto music CDs not only created a weakness in the security of computer systems (later exploited by hackers), it also illustrated the dangers firms face if they attempt to imitate certain outlaw activities for commercial ends. The case illustrated the mismatch between acceptable modes of engagement in mainstream and outlaw activities, and the adoption of covert Black Hat approaches was seen as underhand and a breach of trust between user and supplier, leading to

several class action lawsuits in the US, with similar outcomes emerging from the Intermedia Adware case.

The adaption of outlaw innovations also does not necessarily mean that outlaw users will stop using the original outlaw mods or hacks, nor prevent them from going on to create new ones. The absorption of many outlaw innovations into the mainstream has not prevented new mods from emerging, new product hacks, nor the continued growth of filesharing. This continuing challenge to the mainstream that Outlaw innovation presents will be explored below.

Outlaw innovation as a source of market challenge

Inherent in the nature of Outlaw Innovation is the challenge that it presents to firms via their products, business models and the associated regulatory regimes. Although firms continue to try and appropriate the innovative ideas and other advances that flow from Outlaw Users, their continued presence presents a challenge that can act as a spur to innovation within firms. For example, although we explored how Sony reacted to the hacking of the PSP games console, a similar story could have been told about many other technologies associated with computer games. In this sector, the activities of modders and hackers may have been directly appropriated within the PC games market, but their activities in other product areas have also resulted in firm-led innovations in product architecture and security. It could also be argued that the activities of Black Hat crackers have led to similar innovations in computer security as a whole.

The example of filesharing is unusual in that is presents a challenge both to firms and their business models via the copyright regimes that have been built up around their products and the digital rights management systems they wish users to adopt. Filesharing has developed into a parallel economy that operates outside the mainstream, possesses its own systems of innovation for the generation of algorithms and systems to decode, distribute and access digital content, and has thus far been remarkably resilient to legal and other attacks. This challenge has not only led to the emergence of iTunes and other legal on-line music services, but also initiated a series of structural changes to the music industry and rights management regimes as a whole that have yet to conclude. Outlaw users, including filesharers, may thus be seen as a form of pariah lead user who demonstrate a series of unwelcome market trends that incumbant firms wish to resist.

Outlaw innovation can also be viewed as a form of unregulated market activity in which the needs and wishes of certain types of user are demonstrated in a manner that is unfettered by the limitations that apply to mainstream use. In common with many countercultures it is clearly a transgressive avant garde activity that embraces experimentation (Goffman and Joy, 2004) and is a source of innovation. It represents an environment in which firms are able to observe a high level of activity, some of it innovative, whose motive force emerges from a very different set of drivers than those associated with commercial activity. As such, Outlaw Innovation represents both an alternative source of innovation in its own right, and acts as a counterpoint to structured mainstream user-supplier relationships, potentially driving innovative activity within firms. Certainly, that they are now a large number of knowledge workers or elites available to undertake such experimentation means that such outlaw activity may become a constant feature of the innovation environment within which firms operate.

6 Conclusions

This paper has explored the role and impact of a wide range of ‘hacking’ activities on firm innovation. By focusing on hacking, a phemenon whose impact on innovation is not fully understood, it has sought to extend the existing literature examining the role of the user in firm innovation and the changing nature of the innovation process itself. In developing this discussion the related notions of Outlaw User and Outlaw Innovation were introduced. The relationship between the Outlaw User and the current understanding of the user’s role in innovation was explored and the linkages to the lead user concept were outlined. It was proposed that the emergence of Outlaw Innovation is the result of the same forces that have resulted in

innovation becoming ‘democratised’ (von Hippel, 2005) or ‘Open’ (Chesbrough, 2003), but has found expression as a voice of dissent.

The paper suggested that Outlaw Innovation, at least within IT-intensive digital industries, is the result of widespread activity amongst Outlaw Users, often operating in parallel with commercial activity. The paper argued that such outlaw innovations may be appropriated by firms and acts as an additional source of innovation that may be appropriated, resulting in new and improved products and new markets. A series of cases in which firms had sought develop appropriate responses to Outlaw Innovations were introduced and five distinct organisational responses were identified. Cases in which firms had been either successful or unsuccessful in appropriating Outlaw Innovations were examined and the potential dangers of straightforward imitation were identified.

This paper has outlined the emergence and impact of Outlaw Innovation and the results presented must be viewed as provisional and further research will be required to develop this line of enquiry. It should be recognised that this work will face a number of challenges, both of a methodological and practical nature. Lines of enquiry that may guide further work in this area include: the scale and scope of Outlaw Innovation; the nature of the linkages between firm and Outlaw Users; the impact of Outlaw Innovation in non IT-intensive industries; firm reactions to Outlaw Innovation; the impact of Outlaw Innovation of the direction and path of product innovation; the circumstances in which firms seek to foster Outlaw Innovation activities; the way in which firm responses to this form of activity vary over time and between sector; the conditions under which firms may benefit from an intentioned interaction with outlaw groups. The emergence of such outlaw activities also raises a series of questions for our understanding of innovation including the networked nature of outlaw systems of innovation (e.g. filesharing) and the shifting releationship between users and suppliers. The next stage of this research will be to develop a structured approach to expanding our understanding of this area.

References

AiboPet, 2006a. AiboPet legal controversy - http://aibohack.com/legal/index.html
AiboPet, 2006b. Personal communication, January 2006.
AOL/NCSA, 2004. AOL/NCSA Online Safety Study, www.staysafeonline.info/pdf/safety_study_v04.pdf, accessed on November 25, 2005.
Apple, 2006. iTunes music store downloads top one billion songs, Apple Pres Release, February 23. www.apple.com/pr/library/2006/feb/23itms.html
Au, W.J., 2002. Triumph of the mod, Salon.com. www.salon.com/tech/feature/2002/04/16/modding
Baran, P., 1961. The commitment of the intellectual, Monthly Review, May.
BBC, 2005. PSP embraced by digital technicians, BBC News, April 7, http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/4420745.stm,
BitTorrent, 2006. About BitTorrent, www.bittorrent.com/about.myt
BPI, 2005. Online Music Piracy: the UK Record Industry's response, The British Phonographic Industry Limited, July.
Castells, M., 1996. The Information Age: Economy, Society and Culture, Volume 1, The Rise of the Network Society, Blackwell, Mass.
Chesbrough, H.W., 2003. The Era of Open Innovation, MIT Sloan Management Review, Spring.
Comscore, 2001. Global Napster usage plummets, but new file-sharing alternatives gaining ground, reports Jupiter Media Matrix, Press release, http://www.comscore.com/press/release.asp?id=249 , accessed February 1 2006.
Costello, S., 2000. SDMI cracked? Academics say yes, SDMI say no, Network World, www.networkworld.com/news/2000/1024sdmi.html,
CRIA, 2005. Canadian Recording Industry Association - http://www.cria.ca/filesharing.php
Drucker, P. F., 1959. Landmarks of Tomorrow: a report on the new post modern world, HarperCollins, New York.
Dyer, G, W., Wilkins, A. L., 1991. Better Stories, not Better Constructs, to Generate Better Theory: A Rejoinder to Eisenhardt. Academy of Mangement Journal, Vol. 16, pp613-619.
EFF, 2005. EFF files class action lawsuit against Sony BMG, www.eff.org/news/archives/2005_11.php, accessed on November 25, 2005.
Eisenhardt, K. M., 1989. Building Theories from case study research, Academy of Management Review, Vol. 14, pp532-550.
ELPA, 2005. ELSPA, quoted on DTI website, Computer Games Overview, www.dti.gov.uk/industries/computer_games/ , accessed January 10 2006.
Evers, J., 2005. Sony cracks down on PSP hacks, New.Com, news.com.com/Sony+cracks+down+on+PSP+hacks/2100-1002_3-5885945.htm,
Franke, N. Shah, S., 2003. How communities support innovative activities: an exploration of assistance and sharing among end-users, Research Policy, 32, no 1. Pp 157-178
Freeman, C., 1982. The Economics of Industrial Innovation (2nd Edition), Frances Pinter, London.
Gardiner, P., Rothwell, R., 1985. Tough Customers: Good Designs, Design Studies, Vol. 6, No. 1 p7-17.
GameSpy, 2004. GameSpy's 25 most memorable games of the past 5 years, www.gamespy.com/articles/552/552075p1.html, accessed february 1 2006.
Goffman, K., Joy, D., 2004. Counterculture through the ages, Villard, New York.
Jeppesen L.B., Molin, M.J., 2003. Consumers as Co-Developers: Learning and Innovation Outside the Firm, Technology Analysis and Strategic Management, Vol 15, No. 3.
Jett, D., 2004. Spyware charges levelled at Lexmark, silicon.com, http://software.silicon.com/malware/0,3800003100,39125876,00.htm
Knight, W., 2001. Aibo custom code pulled from website, New Scientist, October 30.
Kuchlich, J., 2005. Precarious Playbour: Modders and the digital games industry, Fibreculture, issue 5, September.
Kushner, D., 2002. The Mod Squad, Popular Science, July.
Levy, S., 1984. Hackers: heroes of the computer revolution, Doubleday, New York.

Lessig, L., 2004. Free Culture: how big media uses technology and the law to lock down culture and control creativity, The Penguin Press, New York.
Livingston, P., 2001. The watermark war, InfoWorld, www.infoworld.com/articles/op/xml/01/05/21/010521oplivingston.html,
Manjoo, F., 2001. Aibo owners biting mad at Sony, Wired News, www.wired.com/news/business/1,48088-0.html
Markoff, J., 2005. What the Dormouse said: how the 60s counterculture shaped the personal computer industry, Viking Books, London, p86.
McCullagh, D., 2005. Senators target 'graphic' video games, new.com.com ; news.com.com/Senators+target+graphic+video+games/2100-1043_3-5975913.html?tag=nl ; accessed January 11, 2006
Microsoft, 2006. Avalanche: file swarming and network coding, Micosoft Research, research.microsoft.com/~pablo/avalanche.aspx
Moddb, 2006. moddb media kit, misc.moddb.com/mediakit/ , accessed Jan 10 2006.
Mollick, E., 2005. Tapping Into the Underground, MIT Sloan Management Review, Summer, pp21-24.
MSN, 2005. Texas sues Sony BMG over anti-piracy software, MSN network, http://msnbc.msn.com/id/10141840/, accessed November 25, 2005.
Niccolai, J., 2005. Microsoft readies Bittorrent alternative, Infoworld.com, www.infoworld.com/article/05/06/16/HNmsbittorrent_1.html ; accessed January 18 2006.
Nuvolari, A., 2004. Collective invention during the British Industrial Revolution: the case of the Cornish pumping engine, Cambridge Journal of Econmics, 28, no 3, pp347-363.
Postigo, H., 2003. From Pong to Planet Quake: post-industrial transitions from leisure to work, Information, Communication & Society, Vol 6. No 4, pp593-607.
Rosenberg, N., 1982. Inside the Black Box: Technology and Economics, Cambridge University Press.
Rothwell, R., Freeman, C., Jervis, P., Horsley, A., Roberston, A.B., Townsend, J., 1974. SAPPHO-Updated; Project SAPPHO Phase II, Research Policy, Vol. 3, Issue 3, pp258-291.
Sharma, D., 2005. Sony adds web browser to to PSP, August 24, http://news.com.com/Sony+adds+Web+browser+to+PSP/2100-1043_3-5842525.html
Sheriff, L., 2005. Enter avalanche: P2P filsharing from microsoft, The Register, www.theregister.co.uk/2005/06/16/filesharing_microsoft.
Stoll, C., 1989. The Cuckoo's Egg, Doubleday.
Takahashi, D., 2005a. Attorney takes on Elecgtronic Arts for "The Sims 2" Nakes Mods, blogs.mercurynews.com/aei/2005/07/attorney_takes_.html ; accessed January 11 2006.
Takahashi, D., 2005b. Game modifiers represent a wide pool of free talent whose ideas have sometimed yielded monster hit – but also controversial twists, Mercury News, July 29.
Tang, P., 2005. Digital copyright and the "new" controversy: is the law moulding technology and innovation?, Research Policy, Vol 34, pp852-871.
Teece, D., 1986. Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy, Research Policy, Vol 15, pp285-305.
Thomke, S., von Hippel, E., 2002. Customers as Innovators: A New Way to Create Value, Harvard Business Review, April, pp74-81.
Toffler, A., 1980. The Third Wave, William Morrow.
von Hippel, E., 1986. Lead Users: A Source of Novel Product Concepts, Management Science, 32 (7), July, pp791-805.
von Hippel, E., and Katz, R., 2002. Shifting Innovation to Users *via* Toolkits, Management Science, 48, (7) July, pp821-833.
von Hippel, E., 2005. Democratizing Innovation, The MIT Press, Cambridge Mass.
Ward, M., 2005. Warcraft game maker in spying row, news.bbc.co.uk/2/hi/technology/4385050.stm, accessed on November 25, 2005
Yin, R. K., 1989. Case Study Research: Design and Methods, Sage Publications, London.

Table 1 : examples of Outlaw Innovation activity

		Sources
Sony Aibo	The Sony Aibo is a toy robotic dog that when it was released in 1999 had a relatively limited set of functions and actions. From late 1999 an individual product hacker, subsequently known as "AiboPet' in the media, began to developing and releasing software tools and extensions to the software supplied with the Aibo. Between the years 2000-01 AiboPet continued to release software via his website that improved the functionality of the Aibo and tools that enabled other users to reprogram their Aibos. Notable among these releases was a piece of software called 'Disco Aibo' that enabled the robot dog to dance to music. By October 2001 Sony had sent several letters to AiboPet expressing their continued concerns and requesting the removal of a series of files from the website. In protest, AiboPet closed down the disputed parts of his websites (AiboPet.com and AiboHack.com). Following the closure of these websites the case was widely discussed in the media (the contents of both letters were published) and AiboPet received significant support from Aibo owners and many others. Sony subsequently withdrew its objections and AiboPet.com was put back online. In 2002 Sony shifted it position and embraced a more open approach to users, initially publishing the software specifications to the Open-R architecture used by the Aibo and making available a software development kit. This was followed in 2004 by the release of the Aibo Software Development Environment (SDE), a suite of tools that were very similar to those developed earlier by AiboPet and designed to enable a wide range of users to develop their own software and included a Motion Editor designed to enable users to create dance routines. Access to this system required users to register, but the Aibo SDE was made available at no charge and registration provided access to the developer website which contained a download area, FAQs and a developer bulletin board.	Knight, 2001 Manjoo, 2001 Lessig, 2004 Aibopet, 2006a Aibopet, 2006b
SDMI competition	In 2000 The Secure Digital Music Initiative, backed by a consortium of firms involved in the provision of digital content, ran a competition to see if external hackers or researchers could crack the digital audio watermark technologies that they had developed. The competition, called the 'Hack SDMI Challenge' offered a $10,000 prize for cracking the encryption technologies, but required participants to sign a non-disclosure agreement in order to claim the prize. A number of groups claimed to have successfully hacked these technologies, including a group of academic researchers who went on to publish their findings and methods.	Livingston, 2001 Costello, 2000 Tang, 2005
Sony PSP	The Sony PSP (PlayStation Portable) is a handheld version of the hugely successful PlayStation 2 gaming platform. Launched in early 2005 it became a magnet for product hackers who exploited flaws in early versions of the PSP firmware. Released without a web browser an early hack was to utilise a browser contained within a computer game, with other hacks including such things as emulators for other gaming platforms (Nintendo), downloading TV shows from a TiVo, and a wide range of applications including PDA software, a virtual drum machine, streaming internet radio, a calculator, and a utility for converting PC video files to PSP format. Sony responded to the hacks by releasing a series of software patches and upgrades to the PSP firmware, including a web browser optimised for the platform and its own website which provided a range of downloadable content. With each new release of firmware flaws that had been exploited by hackers were fixed, and the latest firmware examined for further bugs by product hackers, which were in turn resolved in the next firmware release. Although users were not compelled to install the latest release of the firmware, all new PSP games required the update in order to run. Sony confirmed that they were responding to PSP hacks by updating firmware and were not 'actively going after the people doing it'	BBC, 2005 Evers, 2005 Sharma, 2005
BitTorrent	BitTorrent is a novel P2P file sharing protocol that relies upon the cooperative distribution of the files within the user group trying to download it. With this protocol, the larger the number of people that try to download a file the faster downloading becomes, making it particularly suitable for transferring large files to large numbers of users. In BitTorrent terminology such large groups are called swarms and servers are set up to keep track of the active swarms. BitTorrent tracker sites have been created for the primary purpose of offering copyright material like music and DVDs and some sites have been closed down as a result of legal action, BitTorrent is also widely used for legal file transfer purposes (e.g. distribution of films, software, music, computer games) and, as a result, has thus far avoided legal action. Although Bittorrent has been very successful and is widely adopted it lacks mechanisms for digital rights management and in 2005 Microsoft announced that it was developing a protocol (code-named Avalanche) that is similar to Bittorrent but embodies strong digital rights management facilities.	Niccolai, 2005 Sheriff, 2005 Bittorrrent, 2006 Microsoft, 2006