5. Modchips

How Hardware Hacking Constitutes Grey Markets, User Participation, and Innovation

Mirko Tobias Schaefer

User Appropriation

When a company releases a software application or a software-based product it often actually enters a new phase of development. Skilled users will modify, change and develop the technology further, to suit it to their needs or they might even adapt it for completely different uses, uses which are often unintended and unimagined by the original developer. For most software-based electronic consumer goods one will find easily modifications and related developer communities online.[1]

Video game consoles and their handheld equivalents are extremely popular consumer devices and constitute a valuable and highly contested market. The business models of video game consoles revolves around generating revenues from licenses for third-party developers, selling add-ons for the console such as controllers, remote control and other devices. Increasingly, access to network services and virtual goods become important in generating revenues. The hardware costs provide little or no margin for revenues and often even require vendors to subsidize the initial purchase for the customer. Therefore any appropriation that bypasses the possibilities of generating revenues from licensed software and other add-ons is critical for the vendors. However, users quickly appropriate the design through hacking and reengineering in order to modify the consoles and to execute other than vendor-approved software, and also to play copied games. From playful do-it-yourself modification and homebrew software development to professionalized production of modified processors, so-called modchips, game consoles constitute the emergence of an entire ecology of developer communities, web platforms, production and distribution channels for modified and further developed devices. It led to the emergence of a grey market for modification so-called modchips that enable users to circumvent the original design limitations.[2] This article describes the dynamic interactions between companies, gaming enthusiasts, hackers, and modchip producers in a grey market.

When Microsoft entered the heavily contested market for video game console with its Xbox in 2001, it quickly found the console to be hacked and modified (Huang 2002, 2003; Takahashi 2006, 56-59; Schäfer 2011, 82). The technical specification matched a small computer, which does not come as a surprise given Microsoft's background as the market leader for PC operating systems.[3] A quickly emerging scene of various communities with the most different motives for hacking the Xbox went to work. A group of dedicated Linux enthusiasts, called Xbox Linux Project tried to port the open source operating system onto the proprietary hardware. Other teams focused on developing so-called homebrew software, self-made applications that were not provided by Microsoft.[4] Xbox Media Center became one of the most popular applications for the Xbox, turning the game console into a fully fledged media center for films, video clips, music, and, of course, games. It supports the archiving of media files on the Xbox's hard drive. Other developers provide games or emulate those from outdated platforms for the Microsoft game console.

But in order to do so, the users had to bypass the Microsoft security features that allowed solely the execution of vendor-approved software. The box had to be modified. In general there are two possibilities to modify an electronic consumer good, either through adding a piece of modified hardware, that bypasses or overruns the original processor or a piece of software that adapts the preinstalled firmware. For both solutions, the "hard-mod" or the "soft-mod," the original device needs to be analyzed concerning eventual exploits that can be used to overrun the system and to execute other than vendor-approved code. Walt Scacchi describes the modification of game consoles as

> an expression of game players who are willing to forego the "protections" and quality assurances that console developers provide through product warranties, in order to experience the liberty, skill and knowledge acquisition, as well as potential to innovate, that mastery of reverse engineering affords. (Scacchi 2010)

While communities such as the Xbox Linux Project invested great efforts in the development of a so-called soft-mod, an entire market for so-called modchips emerged. A modchip is a device that is frequently used to circumvent the limitations implemented by the vendor and it allows to execute any software code, including copied games.[5] Producing and distributing modchips as well as the actual practice of modifying a game console has been criminalized in a global and concerted action of the leading manufacturers, Microsoft, Sony and Nintendo. These corporations took considerable effort to represent modchips and their distribution as intellectual property infringement. Through framing it as piracy and exaggerating the potential harm through claiming that money laundering and even terrorism would be tied to modchip production and distribution and the copying of games the corporations successfully motivated law enforcement to ban these practices and enforce the copyright law. However, a further analysis of the emergence of a grey market for modchips reveals that the problem of modchips is located in the nature of computer technology and the flawed business model employed by the companies, and that practice of hacking video game consoles actually provides innovation.

An Intertwined Ecosystem

In August 2005 ten development kits of the Xbox 360 video game console appeared to be stolen from warehouse in Germany.[6] Development kits are not the off-the-shelf consumer units but are specially designed for licensed third-party producers, such as game developers, to test their software to the technical specificities of the video game console. With only a few weeks to the official market entry of their new game console Xbox 360, Microsoft was immediately on high alert. From industrial espionage to blackmailing, all kind of scenarios appeared to be possible. Mandated by Microsoft, German private investigating firm Prevent AG went to work tracking down the stolen kits. What followed had been quite sensationalized described by mainstream media. Images of the technical components of the stolen kits were posted to the website of the SmartXX team, a group of developers specialized in modification chips for the old Xbox. When Prevent's managing director called upon the help of the Austrian criminal investigation department on Friday, 2 September 2005, he presented the case as very urgent; he painted the potential damage for his clients in very dark colors. Convinced that they are confronted either with a case of blackmailing where the consoles were being held for ransom or with industrial espionage, Austrian investigators managed to receive swiftly the necessary authorization and raided the house of a SmartXX member on Sunday, 4 September. They secured two of the stolen development kits. Simultaneously authorities were investigating traces in Germany and the UK which led to further interrogations and the retrieval of the remaining development kits. It appeared that the total of the stolen devices had been initially delivered by an unidentified person to a gaming shop from where several had been sent to another gaming shop.

From there development kits were distributed to several members of the modding and Xbox hacking scene.

What had started out as an industrial espionage thriller became quickly recognized as a accidental occasion where highly valuable devices where sold to gaming shops and from there to hacking enthusiasts. As one of the involved shop owners said: “It was simply the wow-effect of getting your hands on an unreleased console.” The hackers, apart from earning kudos for being first to open yet another box, were driven by their curiosity to investigate technical design. Microsoft did not press charges and allegedly even paid the hackers’ expenses for lawyers.[7] The report of German police station Siegburg, one of the investigating units, concludes that an organized criminal action appears to be unlikely. “Evidence rather indicates an accidental abduction of the devices.” It remains inconclusive, the report goes on, whether the devices had been delivered to a gaming shop or whether they have been distributed deliberately into the hacker scene to constitute a competitive advantage for an unknown third party.[8]

However, the case of the stolen Xbox 360 development kits reveals a dense network of various participants with different motivation. It shows how intertwined the various participants are. Their actions constitute rather a tangled network than clearly defined entities. Gaming shops were at the time an important entrance point for unskilled users to get their gaming devices modified. Having stolen brand new game consoles, and very unlikely being unaware of their actual design as development kits, the thief probably was simply hoping for potential buyers and approached therefore shops selling gaming devices.

From there the devices trickled down into the scene of hackers and modchip developers. The Austrian member of the modchip-producer team SmartXX was also contributing to the Xbox hacker project Xbox Linux Project, which had no commercial interest in hacking the box. One of the two interrogated English citizens was a member of the prominent modchip team Xecuter. The various scenes of gaming enthusiasts, game console hackers, homebrew software developers, and modchip producers appear to be intertwined; often their websites link to each other, but there are also personal overlaps of individuals contributing to several projects and communities. My earlier research on Xbox hacking showed that communities, modchip developers, and homebrew software developers were widely connected through links leading from community websites to development teams and modchip resellers (Schäfer 2011).[9]

Within this scene it remains a persistent rumor that there are also unacknowledged ties to the game console industry. Common users find information on how to modify a gaming console through community websites such as Xbox-Scene. The web platforms for gaming enthusiasts are also the spaces where hackers and common users meet and can exchange thoughts and ideas. Webshops distributing modchips often advertise their services on community websites. Reviews of modchips as well as complete tables which chip matches which console and which version of a vendor's firmware are also posted to community websites.

The possibilities a modded console provides to users has constituted a large demand in modchips. The ability to hack and modify a console has been recognized as a crucial factor in users' decision to purchase an Xbox (Schulz and Wagner 2008, 12). The same seems to be true when looking at the enormous success of devices such as the Nintendo Wii, the PlayStation Portable, or the Nintendo DS. All devices show a dynamic and vivid ecosystem of community web platforms, a large variety of available homebrew software and the Nintendo Wii and Nintendo DS see a steady production and continuous upgrade of modchips. The modification of an electronic consumer-device allows consumers to expand the possibilities of their property and to unlock the actual potential that is provided in the technological qualities of the device but deliberately limited by the vendor through design decisions.

The inherent possibility of modifying the technology or turn it into something different then intended by the original designer called hackers into action. Through reengineering, hacking, and the playful exploit of bugs or insufficient security features, the hackers found possibilities to override the original design and appropriate it. But hacking an electronic consumer device requires skill, time, and dedication many common users do not have. By transforming a hack into a software application or a piece of hardware the tiresome process of hacking becomes formalized and is available as commodity for a larger user group. In the case of modchips, a value added chain emerged, where the domain of game console hackers provides the intellectual labor of hacking and reengineering as well as designing the piece of hardware, which itself will be mass produced and then distributed through web shops.

Zooming into the Grey Market of Modchips

Production

Although their production and distribution often is in violation of intellectual property laws, modification chips are produced on a large scale and respond to user's desire to do different things with gaming devices than the vendors intended.[10] Profound knowledge is necessary to produce a working alternative chip: Knowledge of the specifications of the targeted product, often acquired by reverse engineering the device. It appears natural that enthusiast game console hacking communities of technology-savvy gamers and computer science students show an overlap with the professionalized but yet very informal networks of modchip producers. Those links became visible in the mentioned case of stolen Xbox development kits. However, the level of professionalism of modchip producers is visible in the resources necessary for serial production of a chip.

According to a former member of the modchip producer SmartXX, pre-production can cost up to US$50,000. A former modchip producer revealed that development and production costs can easily add up to US$25 per unit, which are sold for US$28 each. The minimum number of units built for a generation of modchips are approximately 40,000. With sales between 300,000 and 400,000 modchips for the first Xbox, the interviewed modchip producer is estimated to have gained a market share of 35% at the time.[11] This investment and the prospects of revenues force the modchip producers to employ encryption technologies to prevent their hack from being copied by so-called cloners. Cloners are, often Asia-based, producers who simply copy the modchip design and then reproduce it massively. Websites of modchip producers often display warnings about reproductions that allegedly are inferior to the original design.

Producing a modchip is therefore a double cat-and-mouse game. On the one side game console companies try to disable the functionality of modifications through firmware updates which mostly affect so-called softmods, they try to stifle the diffusion through lawsuits against distributors and to adapt the hard- and software of newer versions of their consoles. This often requires the modchip producer to appropriate the initial modification appropriately.[12] On the other side the modchip producer competes with cloners who seek a way to bypass the intellectual labor of reengineering and hacking and attempt to copy the modified design.

In web shops and on developer's websites and community forums are many examples how the modchip producers themselves respond to cloning. The WiiKey for the Nintendo Wii states on its website that it is only original when sporting a hologram. Displaying an "authorized reseller" icon next to the logo of popular modchip producers is another way of winning the consumers' trust. The modchip producers display lists of "authorized resellers" on their own websites. Other websites warn dramatically of potential damages when using a cloned modchip. Similar rhetoric is true for the commercial vendors of the original game console. They also warn users not to modify their devices because it could damage them. "To brick" a game device means that after modification and due to a new firmware update the entire apparatus becomes as dysfunctional as a brick.

Modchip designers attempt to provide a solution for modification that is easy to implement. If the installation of the modchip requires technical skills it could stifle its diffusion. Each new version of a modchip attempts to simplify the process. Modified chips for the Nintendo Wii required soldering. A soldering rod is not necessarily the basic equipment of gaming enthusiasts, and many producers therefore promoted "solderless modding' or emphasize that there are only four cables to solder to predefined solder points. Advertised as "plug and play" chips, the most recent generation of Wii mods do not require any more handicraft work.[13]

Distribution

Modchips are available for all popular consoles, ranging from the Xbox and Xbox 360[14] to the PlayStation 2,[15] Wii, and Nintendo DS.[16] They are mostly available through mail order distributed through webshops and directly through the developers. Developers prefer to ship directly to customers because they can then profit from a higher margin. As a member of the scene said, the majority of the paid market price usually remains with the distributors who demand discounts from the developers. Hong Kong-based mail-order shop Lik Sang had been one of the biggest distributors of modchips for all popular consoles, but had to discontinue this line of business because they lost a lawsuit against Sony over the modchip distribution. Other companies such as Taiwan-based Friend Tech even developed a complete redesign of the original Xbox, and added a new processor, a bigger hard drive and many other features. Countless web shops in Europe and the US distribute modchips for all kinds of gaming consoles. Figure 5.1 sketches the network of modchip distribution.[17] They are mostly modchip resellers, such as Ozmodchips.com, Consolesource.com, Modchipcentral.com, Modnet.no, or Consolepro.nl. Some are solely distributing online, others, such as Gamefreax are both a web shop and an actual brick-and-mortar store. Modcontrol is a community site revolving around modchips.[18] Modchip producer Team Xecuter appears as a well-connected node in the network, and so do the websites representing popular modchips, such as x360usb.com, a Team Xecuter product for modding the Xbox 360, or the Wasabi modchip (wasabi.net.cn) or the WODE Jukebox (wodejukebox.com) for the Nintendo. Clearly visible are the connections of those sites to distributor sites, such as Consolepro.nl, Rejoy.se, Modchipcentral.com, and others.

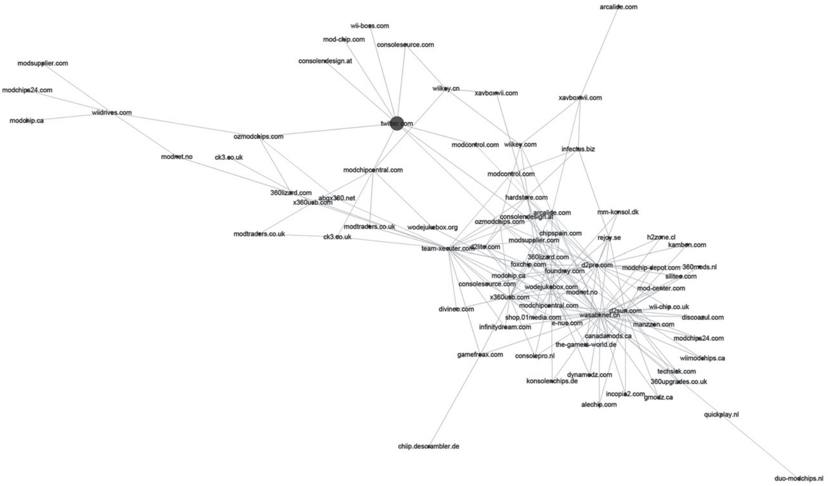

Fig. 5.1: Network of modchip producers and modchip distributors, 2011
(Data collected with Issue Crawler, visualization with Gephi)

An entire grey market has emerged due to the demand for modchips, which are sold in large quantities. The value supply chain starts with the hackers providing the knowledge for a work-around of the original design, and they also develop the design for a modchip, which is then developed through a manufacturer and then distributed through mail order. Modchip producers and distributors are often confronted with legal charges filed by Microsoft, Sony, and Nintendo, who argue that modchips are primarily used for playing copied games.

Warez and Homebrew Software

The main reason for modifying a game console is naturally related to software. This affects four areas of software use: the possibility to produce backup safety copies of the purchased games, the facility to execute nonlicensed software, often called "homebrew software," the circumvention of region codes, and the playing of copied games. Creating backup copies of purchased games is a legal activity as is the creation and use of homebrew software. Attempts to circumvent regional limitations imposed by system of regionally licensed copyrights is a logical consequence of regional price differences in a global market, where users easily can purchase the lower-priced titles online. Reliable figures on download numbers are difficult to obtain; not only are the many industry conducted surveys biased, but retrieving proper download numbers of illegally distributed software is close to impossible to obtain. Surveys use estimates that vary widely.[19] Nevertheless, playing copied games seems to be the prime motivation for game console modification.

Copied games, so-called "warez," are distributed through P2P file-sharing networks and warez servers. Platforms distributing homebrew software therefore deliberately prohibit the distribution of illegal warez through their channels. While the distribution of copied games appears to the original vendors as a direct threat of their business model, homebrew software developers distance themselves explicitly from piracy and rather emphasize the added value their applications provide. Platforms such as DS-Scene.net for the Nintendo DS or the legendary Xbins server for the original Xbox warn their users that they will be banned for any illegal uploads. Consequently homebrew developers do not attempt to monetize their software for the modified devices. A lively homebrew scene had quickly emerged for the original Xbox, the PlayStation Portable and the Nintendo DS, providing many useful applications that expanded significantly the original design. The already mentioned Xbox Media Center allows users to play DVDs from the Xbox, a feature that required – for the unmodified design – the additional purchase of a remote control. The Xbox Media Center did not only turn the Xbox into a media center for video and music files, it also rendered the add-on device, the remote control, obsolete. Very popular software applications for the modified Xbox were the dashboards. A dashboard is a graphical user interface for navigating and operating the various features of the gaming console. A modified console is much more than a machine for playing pirated games, through modification the owner adopts the commodity as her own apparatus, a process that exceeds the predefined options of customizing that companies provide as a pseudo-individual choice.[20]

Commercial vendors try to discourage users from modifying their consoles through stripping them of warranty rights. Microsoft even excludes modified consoles from connecting to its online network Xbox Live and its related services. In 2009 an astonishing 600,000 Xbox 360 consoles were excluded from accessing Xbox Live.[21] In the case of the first Xbox these attempts of excluding modified consoles from the corporate network led to the emergence of completely independent networks such as Xlink Kai. Operating completely beyond the corporate structure, this network even allowed the game consoles of other vendors to connect. A Microsoft Xbox user could play a game against a user operating a Nintendo GameCube. Modchip producers reacted to the latest exclusion of users from the Xbox Live.

Another strategy to prevent exclusion from the network was to build in a switch that allowed the modchip to be turned off when connecting to Xbox Live.[22] While this required quite some tinkering recent modchips for the Xbox 360 provide the turn off option for an Xbox Live-compatible mod. This development is another example for how the modchip producers transform the community-developed hacks into a design feature of a commodity. But quite similar, the commercial vendor can adopt user appropriation to improve the design, as the implementation of many homebrew software applications into the Xbox successor Xbox 360 showed.

Game Console Modding and Its Consequences

As I have explained extensively in my work on participatory culture (Schäfer 2011), the appropriation of corporate design through users meets three different reactions; I have labeled them *confrontation*, *implementation*, and *integration*. Those dynamics are recognizable in the modchip ecology as well. They unfold in a popular and political discourse, in technological design and in legislature.

Confrontation

Confrontation describes the attempts of commercial vendors to label user appropriation as undesirable, illegal, or even dangerous. Additionally, design features aim to stifle user appropriation while the use of intellectual property laws are used to criminalize any appropriation that might endanger the business model. Microsoft's swift reaction to the purloined Xbox development kits is an example for confrontation. Nintendo's lawsuit against Lik Sang's modchip distribution, or Sony's lawsuit against Paul Owen's distribution of the so-called Messiah modchip in the UK show how user appropriation is addressed as copyright infringement (Lim 2008). Accordingly, third-party platforms (such as eBay) outlaw modchips in their terms of use.[23] In their defense, modchip producers and distributors inherently refer to the legendary Betamax case, *Sony Corp. of America v. Universal City Studios, Inc.* (1984), where the court ruled that producers of video tapes can't be held liable for copyright infringement. However, in *Sony Computer Entertainment, Inc. v. Paul Owen & Others* (2002) the court decided that the modchip intentionally provided a circumvention of copyright protection and no exception to infringement was applicable (Lim 2008).[24]

The US Immigration Customs Enforcement (ICE) conducts large-scale operations in order to shut down web shops that trade in modchips. The 2007 "Operation Tangled Web" was one of the biggest raids against the modchip distribution network in the US.[25] Raiding allegedly over 30 locations, the operation was officially targeted against a network of intellectual property piracy. However, many of the websites that were target of the operation, such as Modchipstore.com, are still operating, and many of the alleged businesses for game console modification turn out to be the rather nonprofit activities of skilled game enthusiasts who modify consoles in their local community. While these, often juvenile delinquents, face hefty charges in the US, many web shops remain unaffected from the ICE's activities.[26]

Despite many court decisions that declare the distribution of modchips illegal, it is not difficult to purchase and install these devices, and they are consequently widely used. With their large-scale operations and their quick seizure of addresses that hosts websites used for distributing modchips, copied films, games, etc., the ICE has established herself as the law enforcement arm of the copyright industry.

The copyright industry's influence in pushing for more a more industry-friendly legislature is also visible in international affairs. At least one of the notorious WikiLeaks Cablegate messages addresses the legal status of modchips.[27] The public discourse narrative that is adopted from copyright industry PR is repeated in the public statements of the law enforcement authorities when announcing and justifying their extensive activities against the modchip scene. Former assistant secretary of Homeland Security and Immigration and Customs Enforcement (ICE) Julie L. Meyers stated after the 2007 raids: "Illicit devices like the ones targeted today are created with one purpose in mind, subverting copyright protection."[28] The Homeland Security press release states that modchips stood to cost copyright-holding industries an annual loss of US$250 billion. The figures sketching the alleged losses created through modchips are impossible to verify and can be regarded as completely made up (Schäfer 2011, 134).

The copyright industry (that is, the software, music, and film industries) have developed a reputation for supporting their argument with dodgy figures and biased research (Patry 2009, 30-34; Goldacre 2009). What is visible in the press statements of the ICE and other law enforcement authorities, as well as in the rhetoric used by politicians to set an agenda for a tighter copyright law enforcement and Internet regulation, is actually the spin of the copyright industry.

Using all platforms of public discourse to describe the rather natural process of copying files as criminal activity, the copyright industry defends a system of media content control drawing from the industrial age. However, as Patry has pointed out convincingly for the music industry, this moral panic is created to divert attention away from a business model unfit for a digital economy (2009). This is partially true for the game console producers as well. However, there is an interesting observation to make. While the game console companies engage in concerted activities against the modchip production, they do not completely follow the music industry's hysteric approach. The moral panic displayed in public discourse is more cautious. The game console vendors might be even aware of the benefits of providing a hackable product: A hackable console is more attractive to users and can simply through this accidental feature gain a higher market share (Schulz and Wagner 2008). Other positive side effects of piracy could be the reduction of taxable revenues and the increase of tax allowance for losses created through illegal downloads (Scacchi 2010, 13).

There is even evidence that homebrew software draws at least the interest of corporate software developers (Schäfer 2011). There are persistent rumors within the community of game console hackers that the Xbox development kit of the original Xbox 360 console might have been leaked deliberately into the community. There is no proof for an explicit cooperation between hackers, homebrew developers, and the corporate decision makers. But the dynamics of implementation and integration show that corporations do learn from user appropriation.

Implementation

As implementation, I describe the process of successfully implementing user activities into software design and new business models. The Xbox 360 implemented many features that have initially emerged as homebrew software applications. Microsoft shipped the Xbox 360 with an implemented development kit that turned any user into a legal third-party developer and with its online network marketplace, Microsoft also provided a distribution platform. The lively homebrew software scene that developed hundreds of applications for the original Xbox withdrew almost completely from the Microsoft platform with the advent of the Xbox 360.

While the participation of those developers might have been rendered obsolete through providing many equivalents of the applications that have been initially produced as homebrew software, other reasons for the dwindling interest of hackers and programmers into the Xbox might have been Microsoft's.NET software framework that appears to be unattractive for developing applications as several members of the former developer's scene expressed. They also find a mandatory fee to pay for distributing applications for free through Microsoft's marketplace deeply unattractive. Hacking the Xbox 360 took quite some time but was eventually achieved and modchips are available as well.

Integration

The process of integration is not yet adopted in the area of video game consoles. Integration describes a collaborative effort of company and community to cocreate a commodity. Often this commodity is available for free, such as Google Maps. Here, Google provides an infrastructure and a set of technologies and enables its users to employ their data and geographical mapping information for further uses. The community participates through developing the application further and therefore improves it significantly. This has been described convincingly and in detail, supported by a large number of example cases that the active participation of users benefits the corporate effort and improves and even innovates the original design. The computer game industry integrated user participation through providing editing tools for game modification (Nieborg 2005; Nieborg and Van der Graf 2008). The game industry insists that any derivative of their games is still protected by their copyrights and therefore successfully prevents a commercial exploitation of game mods. This is similar to homebrew software that as unlicensed software cannot be sold.

Apple succeeded in integrating user appropriation into its smartphone platform iPhone by setting up the app store. While Apple grants users the freedom to develop software applications and to distribute them even commercially through the corporate network, they reserve the unlimited possibility of monitoring and regulating the user's productions.[29] Maybe smartphones can serve as an example for the video game console of how to integrate users. That would require the gaming console vendors to rethink their business model and to monetize the gaming platform differently than through licenses.

Prospects of a Grey Market

Since 2005 some things have changed in the modchip universe. The aspect of installing a piece of hardware has been altered to an extent where it is even for novice users possible to modify a game console. While gaming equipment shops have not only been the primary resellers for modchips, they have also been the first address where a user would turn to for game console modification. With the latest generation of modchips and flashcards, modifying a game console became significantly easier. Even novice users are now able to do that.

What script kiddies are to hackers, flashers are to the professional "tuner." Common users now offer modification at a much reduced cost and they advertise it in user fora, promoting their services in the signature of their postings. Websites such as the German Wer-Flasht-Wo.de (translation: Who-flashes-where) provide address lists per region in order to help users find the nearest skilled user to get help with tuning their gaming device.[30] The brick-and-mortar retailers who provided the modchip installation service see themselves as being prevented from delivering a service that generated steady revenue as well as becoming a target for legal action. Since they run official businesses and pay taxes, they can easily be held responsible for the items they sell. Securing their market one cease-and-desist note at the time, the big corporations send their lawyers to muscle the shop owners out of the market. With each note another item will be removed from the range of products. The service of modification is increasingly taken over by teenage users helping other users for some extra pocket money.

The grey market of modchips is in a way a steady companion of the game console market. The user communities, hacker teams, and modchip producers, following various motivations, interact in an environment based on appropriating corporate designs. The strategies used by Sony, Microsoft, and Nintendo show that they do not stand to lose in the dynamic ecosystem that surrounds and accompanies their products. They achieved an almost global prohibition of distributing copied software and managed to criminalize downloads in many countries. Selling modchips as a business has been pushed into the fringes of legality. However, purchasing modchips, downloading pirated games, or modifying a gaming device for whatever reasons remains an easy thing to do. Nevertheless, there are benefits to the modchip universe. Not only might hackability lead to a higher market penetration, an active and enthusiastic community of skilled users actually serves as an extended research and development department to an alert company. The biggest burden for the companies is an ill-suited business model depending on licenses for games rather than revenues generated from the gaming platform itself, related services, and access.

Notes

1. Modifications of the electronic vacuum cleaner Roomba can be found at Roomba robotic vacuum cleaner (www.roombacommunity.com); a Linux operating system for the iPod hacked (http://ipodlinux.sourceforge.net); Aibopet provides the AIBO community with modifications at (http://www.aibohack.com); a forum for PlayStation Portable mods is PSPmod (www.pspmod.com). For almost any device an online forum for modifications is available.
2. Modchip is colloquial for "modification chip." Modchip allows users to execute any software on a game console, including copied games.
3. The Xbox was equipped with an Intel Celeron 733 MHz processor, 64 MB of RAM, an 8 or 10 GB hard disk, a DVD drive, and a network interface, and a stripped-down version of the Windows 2000 kernel served as its operating system.
4. The term "homebrew software" refers to software that was not programmed by a regular company but by members of user communities. Very active platforms for homebrew software are PSP Hacks (www.psp-hacks.com), PSP-Scene (http://pspscene.net/forums/) for the PlayStation Portable, and DS-Scene (www.ds-scene.net), for the Nintendo DS.
5. Modchips are available for almost all common video game consoles.
6. All information about the SmartXX case are retrieved by the author through interviews with several persons involved in the case, either as defendant or investigator. The author further more received a file consisting of documents (e-mail exchange between the private investigators and police authorities; interrogation files, memos and protocols from the German and Austrian authorities). The file has been sent anonymously to the author. In interviews with members of the modchip scene, as well in interviews with detectives participating in the investigation, the contents of the documents could be verified.
7. A statement by SmartXX forum administrator Hamptitampti claims that Microsoft is paying their lawyers and has withdrawn from pressing charges; see "Stolen 360 Developer Kits, SmartXX Speaks Out," post, Xbox360Info.com forum, 5 October 2005, http://www.xb360info.com/xbox/news/168.
8. From the concluding report on the case (Vermerk, 28 November 2005, Landrat Siegbrug, Kreispolizeinehörde). Translation by the author. The document is part of an anonymously delivered zip file consisting of various documents about this case.
9. The research published in Schäfer 2011 includes case examples of modifications of the Microsoft Xbox and the Sony AIBO; the projects on which the research focused date from 2005 to 2008.yyy
10. Karaganis emphasize that no figures and research are available that sketch the actual size of the modchip market. Their writing implicates that the in-

dustry's claims concerning financial losses caused through modchips might exaggerate the actual diffusion of modchips (2011, 50-51).

11. These figures relate to the modchips for the original Xbox. It is noteworthy that these figures are quite different from those reported by Karaganis, who refers to 60,000 modchips that have been confiscated during Operation Tangled Web, the biggest law enforcement operation against modchip distributors in the US (Karaganis 2011, 50).
12. A good example for the changes in game console and the effect on modchip production is the overview of existing Wii modchips at Wikipedia: http://en.wikipedia.org/wiki/List_of_Wii_modchips.
13. FlatMod, FlatMii, Wasabi DX, WiiKey Fusion, DriveKey, and the WODE Jukebox.
14. Known teams of Xbox modchip producers are: Aladdin Chip Team, Duo X2, OzChip Team, SmartXX, Team Omega, Team OzXodus, Team SpiderXS, Team Xecuter, Team X-Changer, Team X-Chip, and Team Xodus.
15. Well-known teams of PlayStation 2 modchip producers include: Infinity Team, Matrix Infinity, Messiah Team, Modbo Team, MXL2 Team, Ninja Team, and Ripper Team.
16. Nintendo DS modchips.
17. For recent mapping of the modchip resellers I assembled a list of modchips from various gaming community sites, such as Xbox-Scene, and from Wikipedia. Using the websites of modchip producers as starting points a crawl with the issue crawler (Rogers) produced a list of websites linked to the initial list of modchip producers. The network mapping was then created through a visualization in Gephi.
18. Note that this crawl is only representing a fraction of the actual reseller market. Somehow many links are ignored, or not taken into account due to absence in the sample of starting points.
19. For a critical analysis of the industry-presented figures, see Julian Sanchez, "750,000 Lost Jobs? The Dodgy Digits behind the War on Piracy," *Ars Technica*, 7 October 2008, http://arstechnica.com/tech-policy/2008/10/dodgy-digits-behind-the-war-on-piracy/. For a thorough analysis of file sharing and record sales, see Felix Oberholzer and Koleman Strumpf, "The Effect of File Sharing on Record Sales: An Empirical Analysis," *Journal of Political Economy* 115.1 (2004): 1-42.
20. Although this chapter discusses only modchips it is important to mention that users also modify the cases of their gaming devices. This case modding is also provided professionally and therefore constitutes another niche in the ecology of gaming consoles.
21. "Microsoft Disconnects Xbox Gamers," *BBC News*, 11 November 2009, http://news.bbc.co.uk/2/hi/8354166.stm.
22. See a tutorial by Captain Dunsel posted to Xbox-Scene: "Adding Mod Chip Enable/Disable and BIOS Flash ROM Write Enable/Disable Switches to Your XBox (v0.6)," http://www.xboxscene.com/articles/endisable.php.

23. See eBay policies: http://pages.ebay.com/help/policies/mod-chips.html.
24. Intellectual Property Case Search System: http://www.ipo.gov.uk/ipcass/ipcass-alphabetical/ipcass-alphabetical-o/ipcass-sony.htm.
25. "Fed's Mod Chip Raid Ended a $2.5 Million Piracy Operation," *Game Politics*, 24 November 2008, http://www.gamepolitics.com/2008/11/24/feds039-mod-chip-raid-ended-25-million-piracy-operation.
26. "Cal State Student Arrested for Playing Video Games," *NBCDFW News*, 7 January 2010, http://www.nbcdfw.com/news/tech/Cal-State-Student-Faces-10-Year-Prison-Term-for-Playing-with-Video-Games-52386872.html.
27. In a 2004 court ruling in Spain modchips had been declared legal, a decision that is discussed in a memo entitled "Aberrant Mod Chip Ruling." The memo expresses concerns that such a ruling might be trendsetting and concludes that the transposition of EU directives on copyright law in Spain will be observed carefully. Retrieved from Cablegatesearch.net: http://www.cablegatesearch.net/search.php?q=%22mod+chip%22andqorigin=oandsort=1.
28. "Crackdown on Modchip Sellers," *BBC News*, 2 August 2007, http://news.bbc.co.uk/2/hi/technology/6928177.stm.
29. This is also true for Google and its Android platform marketplace.
30. Wer-Flasht-Wo.com: http://www.wer-flasht-wo.com.

Bibliography

Bastian M., S. Heymann, and M. Jacomy. 2009. "Gephi: An Open Source Software for Exploring and Manipulating Networks." *International AAAI Conference on Weblogs and Social Media*.

Huang, Andrew. 2002. Keeping secrets in hardware: The Microsoft Xbox case study. MIT AI Lab Memo. http://web.mit.edu/bunnie/www/proj/anatak/AIM-2002-008.pdf.

Huang, Andrew. 2003. *Hacking the Xbox: An Introduction to Reverse Engineering*. San Francisco, CA: No Starch Press.

Goldacre, Ben. 2009. "Illegal Downloads and Dodgy Figures." *The Guardian*, 5 June. http://www.guardian.co.uk/commentisfree/2009/jun/05/ben-goldacre-bad-science-music-downloads.

Karaganis, Joe, ed. 2011. "Rethinking Piracy." In Joe Karaganis, ed., *Media Piracy in Emerging Economies*. New York: Social Science Research Council.

Lim, Yee Fen. 2008. "New hope for consumers of digital copyright material in Hong

Kong." In Brian Fitzgerald, Fuping Gao, Damien O'Brien, and Sampsung Xiaoxiang Shi, eds., *Copyright Law, Digital Content and the Internet in the Asia-Pacific*. Sidney: Sydney University Press.

Nieborg, David B. 2005. "Am I Mod or Not? – An Analysis of First Person Shooter Modification Culture." Paper presented at Creative Gamers Seminar – Exploring Participatory Culture in Gaming, Hypermedia Laboratory, University of Tampere, Finland. http://www.gamespace.nl/content/DBNieborg2005_CreativeGamers.pdf.

Nieborg, David B., and Shenja van der Graaf. 2008. "The Mod Industries? The Industrial Logic of Non-Market Game Production." *European Journal of Cultural Studies* 11.2: 177-195.

Patry, William. 2009. *Moral Panics and the Copyright Wars.* Oxford: Oxford University Press.

Scacchi, Walter. 2010. “Computer Games, Mods, Modders and the Mod Scene.” *First Monday* 15.5, 3 May. http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2965/2526.

Schäfer, Mirko Tobias. 2011. *Bastard Culture! How User Participation Transforms Cultural Production*. Amsterdam: Amsterdam University Press.

Schulz, Celine, and Stefan Wagner. 2008. “Piracy and Outlaw Community Innovations.” *International Journal of Innovation Management* 12.3: 399-418.

Takahashi, Dean. 2006. *The Xbox 360 Uncloaked: The Real Story Behind Microsoft’s Next-Generation Video Game Console*. N.p.: Spiderworks.