

# Architectures of Control in Consumer Product Design

Daniel Lockton : MPhil Technology Policy : June 2005  
Judge Institute of Management : University of Cambridge

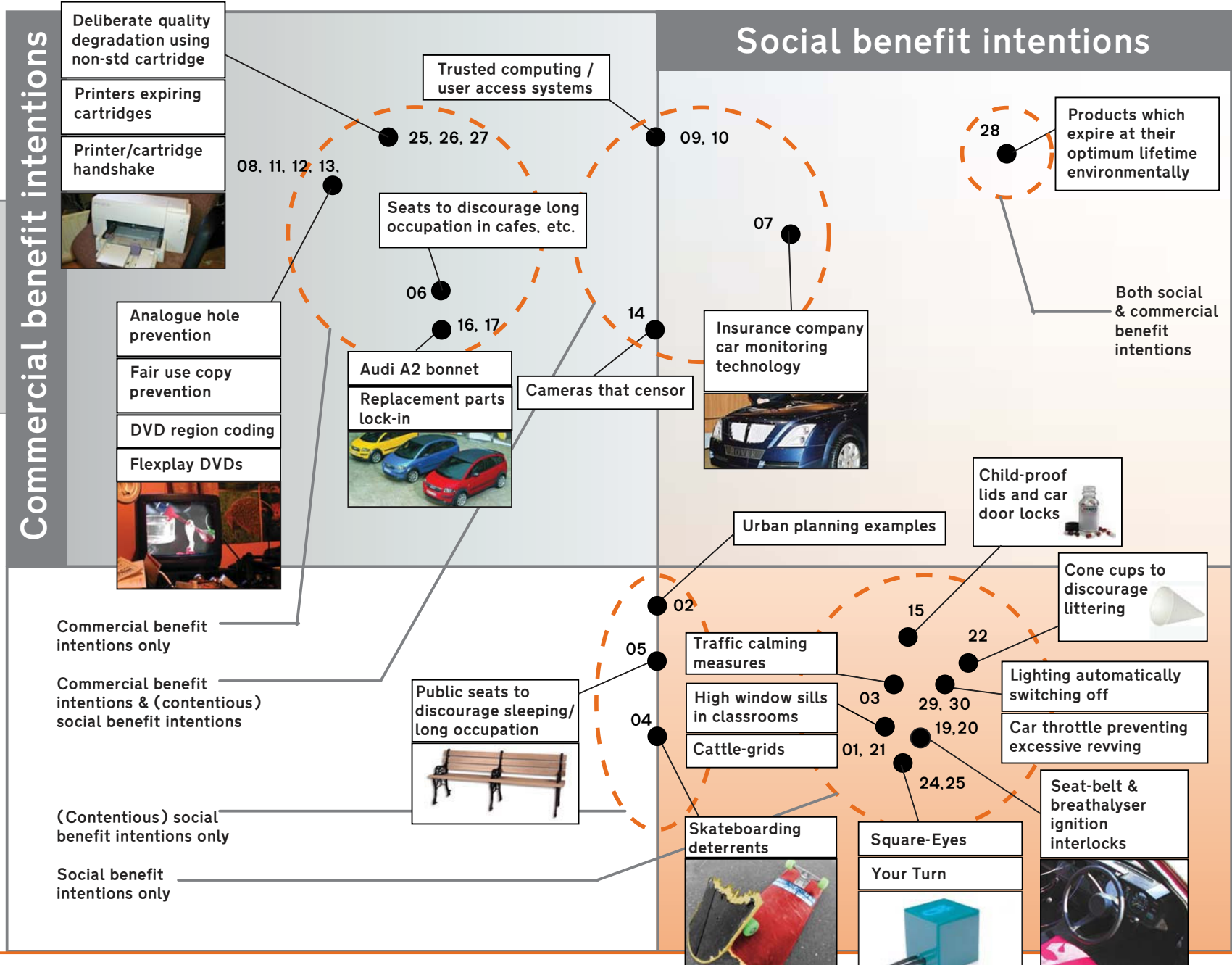
---

This is a slightly modified version (v.1.01) of the paper as submitted. Comments are very welcome:  
[dan@danlockton.co.uk](mailto:dan@danlockton.co.uk). Thanks.

Supervisor: Dr David Reiner

---

Diagram:  
The strategic intentions behind some architectures of control discussed in this paper. See page 19 *et seq.*, 'Summary of examples' and the case studies.



## Contents

Abstract	1	Reactions	
Introduction	1	The technical community	23
The range of architectures of control:		Consumers: DRM	26
The built environment		Consumers: external control	29
Urban planning	2	Some implications	33
Disciplinary architecture	3	Conclusion	38
The digital environment		References*	39
Digital rights management	6	Academic precedents:	
Trusted computing	8	Artefacts & politics	3
The analogue hole	9	What things regulate	5
Other digital control	10	Control & networks	11
Simple control in products		Everyday things &	14
Restriction of access	13	persuasive technology	
Forcing functions	14	The democracy of innovation	22
Mistake-proofing	17	Case studies:	
New opportunities	18	Printer cartridges	32
Summary of examples	19	‘Optimum lifetime products’	36
Illustrative representation	<i>Inside cover</i>		

---

## Declaration

“This dissertation is substantially my own work and conforms to the Judge Institute guidelines on plagiarism. Where reference has been made to other research this is acknowledged in the text and bibliography.”

## A note on sources

Where a source is a personal correspondence or discussion, and thus has not previously been published, this is clearly indicated in the list of references. The views of individuals should be taken as personal opinion and are not intended to reflect the official views of the companies or institutions with which they are associated.

*\*This “single separate listing of cited references” is not to be included in the word limit.*

## Acknowledgements

Thanks are due to my supervisor, David Reiner (University of Cambridge), and in no particular order, Frank Field (MIT), Steve Portigal, Andreas Bovens (K.U. Leuven, Meiji University), Bill Thompson (BBC), Cory Doctorow (Electronic Frontier Foundation, BoingBoing), Stuart Constantine (Core77), Chris Weightman (Tangerine), Hamish Thain (Burgopak), Rob Lemos (SecurityFocus), James Howison (Syracuse University), Julian Wood (Active Fasteners), Peter Moar (University of Cambridge), Michael O'Donnell (Brunel University), Paul Turnock (Brunel University), Burak Arikan (MIT Media Lab), David Harrison (Brunel University), Arnaud Bonnet (University of Cambridge, Gown), Tom Clarke (Logica CMG), Megan Meredith-Lobay (University of Cambridge, Gown), Tricia McLaughlin (Downing College), Koranteng Ofosu-Amaah, John Williams, Nigel Olding—and to my family, for suggesting many architectures of control, and keeping me motivated.

# Architectures of Control in Consumer Product Design

---

Daniel Lockton  
Downing College, University of Cambridge  
June 2005

dan@danlockton.co.uk  
www.danlockton.co.uk

---

## Abstract

The idea of architectures of control is introduced through examples ranging from urban planning to digital rights management, and the intentions behind their use in consumer products are examined, with reference to case studies of printer cartridges and proposed 'optimum lifetime products.' The reactions of the technical community and consumers themselves are also explored, along with some wider implications.

---

## Introduction

Architectures of control are features, structures or methods of operation designed into physical products, software, buildings, city layouts—or indeed any planned system with which a user interacts—which are intended to enforce, reinforce, or restrict certain modes of user behaviour.

Whilst the use of architectures of control in computing is well-known, and a current issue of much debate (in terms of digital rights management, 'trusted' computing and network infrastructures themselves), it is apparent that technology is also offering increased opportunities for such architectures to be designed into a wide range of consumer products; yet, this trend has not been commonly recognised.

This paper examines some of these applications, the intentions behind them, wider consequences and future uses of architectures of control. The assumption is made that products and systems can be engineered and designed with rationales and intentions behind them beyond the *prima facie* functionality or appearance requirements of a conventional specification or brief.

## The range of architectures of control: the built environment

First, it is worth looking at the broad range of architectures of control both inside and outside of product design. The use of the term ‘architecture’ is no coincidence, since it is in the planned systems which people inhabit—buildings and environments—that the idea of shaping behaviour is consistently evident.

On a small scale: the high windows of traditional British school classrooms might be positioned in the optimum location for lighting (on the ‘left’ to illuminate the work of right-handed pupils—an ‘accessibility’ debate in itself), but the sills are almost always high enough to prevent pupils’ being distracted by events outside. This is a simple architecture of control.

### Urban planning


On a grander scale: the designs of urban planners such as Baron Georges-Eugène Haussmann [1,2], who remodelled Paris for Louis Napoléon (later Napoléon III) after 1848, may include elements of physical crowd control (replacing many narrow streets—which had made the revolutionaries’ barricades effective—with broad boulevards and avenues [1]) and, less obviously, psychological crowd control (a mob may feel less powerful if positioned in the middle of a large area, whether that be a park or a thoroughfare).

Despite Jane Jacobs’ wise warnings in *The Death and Life of Great American Cities* against generalising about the value of “More Open Space” in city planning [3], as part of an architecture of control it becomes just another tool in the strategic toolbox. Indeed, strategic design may be something of a synonym for the use of architectures of control, not just in ‘political’ city planning—which will be considered further later—but across the range of human endeavour where some particular user behaviour is desired or required.

Extending the review into other aspects of the built environment, features as diverse as ‘traffic calming’ (speed humps, built-out kerbs and chicanes as physical controls, removal of road centre-lines as psychological controls [e.g. 4]), the increasing use of ‘pig ears’ on walls and radiused kerbs as deterrents to skateboarders [5], and even park benches with central armrests [e.g. 6] to prevent people sleeping on them (or indeed, ‘perches’ at bus-stops and deliberately uncomfortable café chairs to discourage lingering), all fall into the category of architectures of control.

## Disciplinary architecture

At this point, the discussion could well move into how what is characterised as ‘defensive architecture’ is in fact ‘disciplinary architecture’; as Ocean Howell of San Francisco State University notes [5], it is ‘defending’ the general public against ‘undesirable’ behaviour by other members of the public.

This is only one step away from Jeremy Bentham’s Panopticon [7] and Michel Foucault’s argument (in *Discipline and Punish* [8]) that by embedding punishment systems in architecture and institutions (e.g. prisons) rather than meting out direct retribution publicly (e.g. public execution or floggings), the likelihood of adverse public reaction to the punishment is greatly reduced. In the park bench example, a public confrontation between police and a person sleeping on the bench (with possible 

### Academic precedents: artefacts and politics

Many academic fields touch on areas relevant to this subject, from architecture to computer science. Perhaps the closest single exposition of many of the pertinent concepts is Langdon Winner’s 1986 “Do artifacts\* have politics?” in which he discusses the idea that:

“The machines, structures, and systems of modern material culture can be accurately judged not only for their contributions to efficiency and productivity and their positive and negative environmental side effects, but also for the ways in which they can embody specific forms of power and authority” [1]

Winner uses examples to show both intended strategic architectures of control, and technologies which have had an unintended political or social effect (but which are not architectures of control). The former category, relevant to this subject, includes Baron Haussmann’s ‘new’ Paris (*q.v.*) and much of Robert Moses’ urban planning in New York City—most notably the low bridges on Long Island parkways to prevent buses (more likely to have poorer users) from travelling to areas such as Jones Beach, “Moses’ widely acclaimed public park”:

“Many of his monumental structures of concrete and steel embody a systematic social inequality, a way of engineering relationships among people that, after a time, became just another part of the landscape” [1].

Concluding by exhorting us to “achieve a clearer view” of the interactions between technology and society, and to consider and understand more fully the consequences of how “specific features in the design or arrangement of a device or system could provide a convenient means of establishing patterns of power and authority in a given setting,” Winner’s work was extremely prescient and the implications are even clearer today.

*\*I have retained the US spelling for this title*

sympathy from bystanders) can be avoided entirely by preventing anyone sleeping on the bench in the first place (using the architecture to control). Not for nothing are speed humps commonly known as ‘sleeping policemen’ in the UK.

Nevertheless, whilst fascinating, it is perhaps counterproductive to go too deep into this vein, since within the context of product design, it is clear that many of the objectives of Foucault’s “technologies of punishment” can be achieved, and even surpassed, through architectures of control—surpassed in the sense that people can be prevented from committing the crimes in the first place.

A breathalyser interlock on a car ignition can stop the crime occurring, thus there is no need for punishment. The necessary discipline is forced on the user by the product architecture. Bentham’s Panopticon guard need not sit in the centre any more to achieve optimum surveillance. He or she could be replaced by a computer monitoring the behaviour of every inmate—or indeed, preventing infractions in the first place, as far as possible.

As another product example of disciplinary monitoring, the Traksure black-box monitoring system for ‘young male drivers,’ offered by AXA Insurance in Ireland [9], records and transmits (via GSM) the car’s speed and location, in return for a discount on the premium for ‘safe’ drivers; a similar system is on offer in the UK, but focused on enforcing a mileage-based insurance policy [10].

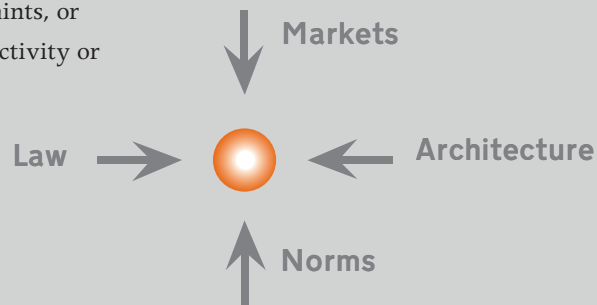
## Academic precedents: what things regulate

Lawrence Lessig, currently of Stanford Law School, has been at the forefront of much recent and current debate on intellectual property and how the internet is constructed and regulated. His books, *Code, and Other Laws of Cyberspace* [29], *The Future of Ideas* [51] and more recently *Free Culture* [26] have established the issues of online freedom, the Creative Commons and the digital rights debate within an academic framework.

Specifically relevant to this paper is Lessig's chapter, 'What things regulate,' in *Code, and Other Laws of Cyberspace*, in which the idea is introduced of four constraints, or 'regulators' on an individual, or an activity or behaviour:

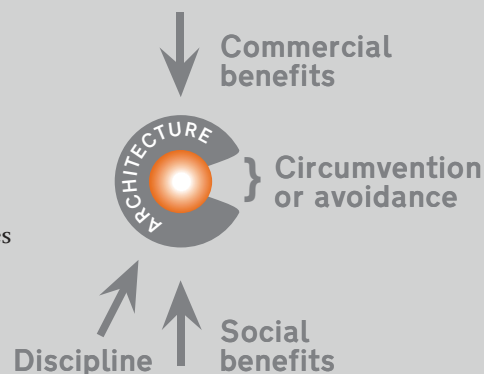
"Four constraints regulate this pathetic dot—the law, social norms, the market, and architecture—and the 'regulation' of this dot is the sum of these four constraints... The constraints are distinct, yet they are plainly interdependent. Each can support or oppose the others. *Technologies can undermine norms and laws; they can also support them [emphasis added]*" [50].

Lessig's four regulators



In a sense, this paper is investigating how the 'architecture' regulator can be (and is being) extended—through the incorporation of architectures of control into products—so that its scope encompasses the aims of the market (commercial benefit) and possibly the law (disciplinary architecture) and social norms (social benefit), although the mapping is clearly not exactly one-to-one:

Possible modification to illustrate architectures of control



Lessig's architecture is applied to the internet in terms of the software that governs the way people and machines can interact; his argument is that governments (or companies) have a range of methods beyond the law itself through which they can regulate consumers' behaviour, and that the public should wake up to this. This paper aims to demonstrate some manifestations of that regulation in the context of product design.



## The range of architectures of control: the digital environment

The design field where architectures of control have become most firmly established is software; to a large extent any application which affords the user a limited range of behaviours is, by definition, an architecture of control.

This may seem obvious, but it is not a trivial statement to make: a system which uses a limited set of algorithms to determine how it functions is different to our experience of the ‘real’ world, in which the rules also exist but are (mostly) too complex for us to analyse deterministically. However, it may be argued that the architectures of control are what gives the software its function in the first place, so it is more useful here to look at the ‘next level up’ of control in software—architectures of control with strategic intentions of some kind.

### Digital rights management

Digital rights management (DRM) can encompass a variety of architectures of control—in the words of Andreas Bovens, “in essence, every use that is not specifically permitted by the content [or hardware] provider is in fact prohibited” [11].

This situation, whilst it has legal precedents in the idea of explicitly enumerated lists of rights (as opposed to a more evolutionary common law approach), has never before been applicable to products. The implications of this level of control for unanticipated ‘freedom to tinker’ innovation cannot yet be fully appreciated, but, as will be examined later, could be significant.

One factor driving DRM’s adoption is that digital electronics permits (indeed, relies upon) exact copies of information being made at low or zero marginal costs. Thus if the information vendors (who may or may not be the rights-holders) wish to maintain their revenues or restrict the availability of information, technology needs to be embedded in the architecture of the information, or copying device, or both, which controls or restricts that ability to copy. DRM allows the balance of control to be shifted from the user (*e.g.* “Who’ll know if I photocopy a book in the library rather than buying a copy?”) to the content or hardware provider (*e.g.* “We’ll build a photocopier that will refuse to copy the book in the first place”). Similarly, then, to the ‘disciplinary architecture’ outlined in the built environment context, DRM, both as copy-prevention and for other purposes, can be used to prevent legal infractions.

However, it can equally be used to prevent behaviours which are by no means illegal, but which the DRM controller desires to prevent for its own strategic reasons—

in some cases, infringing established rights on the part of the consumer. For example, in most legislatures, it is accepted that a backup copy may be made of software, audio or video purchased by the consumer; yet DRM can prevent this ‘fair use’ copying with impunity [12]. Equally, there is the right of a customer to re-sell an item he or she has purchased; this, too can be restricted using DRM, to the extent that, say, software could not be installed on a subsequent purchaser’s machine, even if it had been uninstalled from the original—to what extent this affects the statutory property rights of the purchaser will be an area of increased debate as DRM becomes more prevalent.

There is increasing potential for DRM to provide the architectures of control to enforce the (often very restrictive) end-user licence agreements (EULAs) for software; whilst it is likely [13] that many users do not fully abide by the EULAs to which they currently ‘agree,’ architectures of control embedded in both software and hardware could greatly reduce the possibilities for deviance.

Another implication of some DRM architectures is the control of user access: certain users could be prevented from viewing information or using functions (trivial strategic hardware analogues might be keeping certain items on high shelves to prevent children reaching them, or ‘child-proof’ lids on medicine bottles).

The discrimination could well be purely for security reasons (just as the first encryption of a message was, in itself, an architecture of control), but when a combination of economic and political motivations comes into play, the dystopian science-fiction vision presented back in 1997 in Richard Stallman’s “The Right to Read” does not appear especially exaggerated:

“In his software class, Dan had learned that each [electronic] book had a copyright monitor that reported when and where it was read, and by whom, to Central Licensing. (They used this information to catch reading pirates, but also to sell personal interest profiles to retailers.) The next time his computer was networked, Central Licensing would find out.” [14]

## Trusted computing

Indeed, as the quote shows, Stallman also anticipated the rise of ‘trusted computing,’ in the sense of a computer which will report on its owner’s behaviour and—perhaps more importantly—is built with the ability for a third party, such as Microsoft, or a government agency (“absentees with clout” in Stallman’s phrase) to control it remotely. Of course, any attempt by the user to prevent this would be automatically reported, as would any attempts to tinker with or modify the hardware.

There is insufficient space here to explore the full range of architectures of control which trusted computing permits, but the most notable example identified by Cambridge’s Ross Anderson [15] is automatic document destruction across a whole network, which could remove incriminating material, or even be used to ‘unpublish’ particular authors or information (shades of *Fahrenheit 451*). Users who are identified as violators could be blacklisted from using the network of trusted computers, and anyone who is recorded to be contacting or have contacted blacklisted users would automatically be put under some suspicion.

Within organisations (corporate and governmental), as Anderson points out, these architectures of control could be very useful security features—indeed, perhaps the salient features which spur widespread adoption of trusted computing. Confidential documents could be kept confidential with much less fear of leakage; documents could be prevented from being printed (as some levels of Adobe PDF security already permit [16, 26]); and those who have printed out restricted information (whether they be correspondence, CAD data, or minutes of meetings) would be recorded as such. Sensitive data could ‘expire,’ just as Flexplay’s DVDs [17] self-destruct 48 hours after they are removed from the package (another product architecture of control).

The impact of data expiry on long-term archiving and Freedom of Information legislation, where internal government communications are concerned, is as yet unclear [18]; equally, the treatment of works which are legally in the public domain, yet fall under the control of access restrictions (the Adobe *Alice in Wonderland* eBook débâcle [e.g. 19, 27] being a DRM example) is a potential area of conflict. It is possible that certain works will never practically fall into the public domain, even though their legal copyright period has expired, simply because of the architectures of control which restrict how they can be used or distributed.

The wider implications of trusted computing architectures of control are numerous—including a significant impact on product design as so many consumer

products now run software of one form or another. The network effects of, for example, only being able to open files that have been created ‘within’ the trusted network will work heavily against non-proprietary and open-source formats. Those outside of the ‘club’ may be under great pressure to join; a wider move towards a two-tier technological society (with those who wish to tinker, or have to, from economic or other necessity, being very much sidelined by the ‘consensus’ of ‘trusted’ products and users) is possible.

### **The analogue hole**

The ‘analogue hole’ is another issue which architectures of control in both products and software aim to address. In simple terms, this is the idea that however sophisticated the DRM copy prevention system is on, say, a music CD, the data still have to be converted into an analogue form (sound) for humans to hear. So, if one can capture that sound and re-digitise it (or store it in an analogue form), a near-perfect copy can be made, circumventing any copy-prevention measures. Indeed, digital-to-analogue-to-digital conversion (as used in most modems) has also been used for some innovative reverse engineering, such as extracting the iPod’s firmware as a series of clicks in order to aid the iPodLinux project [20]. With such uses, it is perhaps no wonder that analogue-to-digital converter ICs themselves (ADCs) are considered as “endangered gizmos” by the Electronic Frontier Foundation [21].

Architectures of control to plug the analogue hole could include products which refuse to record any input unless a verified authorisation signature is detected in the signal, or a product which deliberately degrades anything recorded using it (or only provides degraded output for connection to another device). Indeed, a ‘Broadcast Flag’ or equivalent [22], embedded in the signal or content, could explicitly list characteristics of any recording made, such as quality degradation, prevention of advertisement skipping, or number of subsequent copies that can be made.

Extending this idea, cameras and camcorders could detect the presence of copyrighted, trademarked or DRM’d material in an image or broadcast and refuse to record it, thus preventing the use of camcorders in cinemas—but also, perhaps, preventing your hobby of photographing company logos, or, as Cory Doctorow points out, “[refusing] to store your child’s first steps because he is taking them within eyeshot of a television playing a copyrighted cartoon” [23]. A possible extension of this would be cameras or camcorders which would automatically censor certain images for reasons other than copyright—for example, censoring significant areas of flesh.

The issue of the proposed Broadcast Flag [22]—still not resolved at time of writing [e.g. 24]—is another in a series of attempts by economic interests to lobby legislators to incorporate support for architectures of control into law.

The major example in this field is the Digital Millennium Copyright Act (and its worldwide equivalents), which prohibits the development or distribution of technology intended to avoid copy prevention measures [25]; whether this is a genuine attempt to promote creativity through protecting copyright, or just rent-seeking, has been the subject of an enormous amount of debate over the past few years [e.g. 28]. The precedent set with DVD region-coding, for example, suggests that commercial benefit is the only motive of much work in this field, with no benefits for the consumer.

### **Other digital architectures of control**

The architectures of computer networks themselves can, of course, be an important method of controlling user behaviour (and, along with other network architectures, have been studied extensively—as discussed in ‘Academic precedents: control and networks’). Without going into too much detail here, it is clear that much of the growth of the Internet can be put down to very loose, yet still functional, architectures of control, or code, as Lawrence Lessig (*q.v.*) puts it [29]. Anyone is free to write software and distribute it, publish information or ideas, transfer files, contact other users, or interact with and use data in different ways.

Architectures that introduce a more restrictive, prescriptive (and proscriptive) network structure may have benefits for security in online commerce and certainly offer governments a strategic tool for more effective control and censorship. As more and more consumer products operate as part of networks (from computers themselves to mobile phones and even toys), the potential for the network structure to be a significant architecture of control also increases.

Finally, the idea of captology [30], or “computers as persuasive technology”—using features inherent to computer-based systems to persuade users to modify their behaviour (for example, giving up smoking, or increasing motivation to exercise)—is a growing area in itself, and whilst captology always intends to persuade rather than coerce or force, the thinking has much in common with strategic design and architectures of control. Captology is examined further in ‘Academic precedents: everyday things and persuasive technology.’

## Academic precedents: control and networks

To some extent, the desire of companies to control what consumers do with their products has parallels with attempts at price discrimination in industries such as freight transportation, and, especially, telecommunications.

Andrew Odlyzko of the University of Minnesota's Digital Technology Center points out that telecommunications companies are currently able to achieve revenues of \$3,000 per megabyte of data sent through SMS, yet the same data sent through cable TV would yield only \$0.00012 per megabyte [60]. The internet—where, effectively, all data are priced the same—lacks these architectures of control, and this:

“...helps explain the push in the telecommunications industry for new network architectures that would provide service providers greater control of what customers do, and would deviate from the ‘stupid network’ model of the Internet.” [60]

Regulation and control of users' behaviour in other telecommunications networks can also be a commercial necessity, especially where bandwidth is considered to be at a premium—for example, wireless grids, “challenging environments in which users' strategic behaviours are crucial to system performance.” [61]

Lee McKnight, William Lehr and James Howison have reviewed technical, social, legal and economic methods to regulate behaviour in wireless grids (paralleling Lessig's four regulators, *q.v.*), with the technical methods most closely corresponding to architectures of control as examined here—as they put it:

“Appropriate behaviour can be ‘hard-wired’ into the network through hardware and software design... The key is to define open interfaces that provide sufficient assurance as to the functionality that will be supported to allow interoperability without dictating detailed implementation rules that might limit innovation.” [61]

On a similar issue, ‘internet appliances’—the hardware through which a user (or a device) connects to the internet for a dedicated “particularity of purpose”—come into the picture as products for enacting architectures of control on behalf of telecommunications companies or ISPs: since the architecture of the internet itself is difficult to change, control may be put into the components which face the user.

Sharon Gillett, John Wroclawski, David Clark and William Lehr again (all MIT) have examined a range of internet appliances, the architectures of control built into them, and threat posed to “internet innovation” by the devices; their conclusion is that because of the enormous number of existing PCs, largely free of restrictive control, connected to the internet, any new, restrictive device will be at an immediate disadvantage—even if simply because users will be dissatisfied by these devices' lack of forwards compatibility:

“Truly fixed function appliances... are unlikely to place a serious drag on innovation, because they are only likely to succeed in the marketplace if they are inexpensive, frequently replaced devices [e.g. phones]” [62].



Nevertheless, they accept that devices where the function can be remotely changed through automated software updates (such as the TiVo) are more of a risk—but note consumers' lack of enthusiasm:

“Consumers do seem to be quite aware of, and unenthusiastic by, the extent to which high switching costs would lock them into particular devices and services. This kind of lock-in may be a policy issue in its own right, especially if coupled with other products, services, or practices that raise antitrust concerns” [62].

Although not expressly considered by Gillett *et al*, trusted computing would seem to fall squarely into this category, and, assuming that the majority of existing PCs are ultimately replaced by 'trusted' computers, the threat suddenly gains considerable momentum.

## The range of architectures of control: simple control in products

Whilst architectures of control in digital systems can be complex, there are many very simple control architectures in products which are either self-evident, or become so once the design intention is explained.

### Restriction of access

Some of the most obvious involve attempts to restrict access of certain users. At a very basic level, locks and the keys that go with them (whether physical keys, or passwords, or PINs, or biometric identification systems) are architectures of control. But it is child-proof lids on medicine bottles, placing things ‘out of reach of little hands’ and child locks on car doors with which we are most familiar.

Equally, adult users may have their access restricted to particular components for safety reasons, although denying access in this way is often done for economic reasons—a recent example being the bonnet of the Audi A2 which is not intended to be opened by the car’s owner, but only by an authorised Audi dealer. It is presented as a ‘convenience’ feature—and some owners undoubtedly see it this way, for example this quote from an online review:

“You cannot open the bonnet—correct—a specialist has to open it for you—now I don’t know if some of you will think this a disadvantage, but I certainly didn’t! To access the water and oil supply, just flick a switch inside the car, and the Audi logo at the front of the vehicle flips open. There you will have access to fill up water and oil—clever stuff!” [31]

The implications of restricting the ‘freedom to tinker’ (and even the ‘freedom to understand’) in this way will be examined in the ‘Reactions’ section later, but where the economic motive behind an architecture of control is more baldly obvious, such as Hewlett-Packard’s printer cartridge expiry (see ‘Case Study: Printer Cartridges’), some consumer backlash has already started. Nevertheless, there is nothing unusual about economic lock-in; even when purchasing replacement parts for products where only the ‘genuine’ parts will fit (or where non-genuine parts will invalidate a warranty), from razor blades to batteries, we are consistently subject to it, reinforced by branding.



## Forcing functions

On a different note, many architectures of control in products are what Donald Norman calls ‘forcing functions’ (see ‘Academic precedents: everyday things and persuasive technology’)—“actions are constrained so that failure at one stage prevents the next step from happening” [32]. A common way of achieving this is an ‘interlock,’ which could be an aid to usability—to increase the likelihood that the product is operated in the correct order (for example, Steve Portigal suggests a card payphone where the card slot is underneath the handset, thus ensuring the handset is lifted before the card is swiped [33]).

Equally, interlocks can be used for more strategic disciplinary functions—preventing illegal acts by the user, such as a breathalyser fitted to a car’s ignition system such that only when the test is ‘passed’ can the car be started. There are variants of this, e.g. the ‘Simple Simon’ memory game using coloured lights, used on the MG/British Leyland SSV1 ‘safety car’ prototype in the 1970s, which would also deal with overly tired or drugged drivers:

“Get the (randomly generated) sequence wrong three times in a row, and [the driver] would have to wait an hour before being allowed to try again. While designed primarily as a safety device, this feature also doubled as pretty effective immobiliser.” [34]



### Academic precedents: everyday things and persuasive technology

Two precedents from the interface between design, business and psychology are especially relevant here.

First, Donald Norman’s influential *The Psychology of Everyday Things*, later republished as *The Design of Everyday Things* [32], formalised and analysed much of the accumulated wisdom surrounding user behaviour and interaction with products—taking ‘human factors’ design beyond ergonomics and anthropometrics and into the field of usability: considering users’ conceptual models and

mental processes, with the aim of improving the customer experience (and, with it, making products more competitive in the marketplace).

Norman’s clear explanation of forcing functions—he uses the seatbelt interlock as an example—with the classification into interlocks, lock-ins and lock-outs, is useful as a framework for understanding many architectures of control. He also sounds the appropriate notes of caution for designers considering the use of forcing functions:



“If a forcing function is really desired, it is usually possible to find one, although at some cost for normal behaviour. It is important to think through the implications of that cost—to decide whether people will deliberately disable the forcing function... It isn’t easy to force unwanted behaviour onto people. And if you are going to use a forcing function, make sure it works right, is reliable, and distinguishes legitimate violations from illegitimate ones” [32].

The other major precedent at this design-business-psychology interface is the work of B J Fogg and his team at Stanford’s Persuasive Technology Laboratory [52] into ‘captology’—computers as persuasive technology. Whilst much of the work is concerned explicitly with computer-based persuasion (websites, games and interactive software), the extension of software into products, particularly mobile devices is also a component of the research.

Fogg is explicit about the distinction between persuasion and coercion (and deception); many (indeed most) of the architectures of control outlined in this paper would undoubtedly be classed as coercive technology rather than persuasive technology by his definition.

For example, taking two products which have a common possible outcome (reducing the amount of hours for which children watch television), Square-Eyes (*q.v.*) is probably on the coercion side of the boundary, whilst the AlternaTV system mentioned in Fogg’s book *Persuasive Technology* [53] is on the persuasion side, since it does not actually restrict children, merely encourage them through, effectively, a competition to see which ‘team’ can watch the least television.

Nevertheless, many of the points that Fogg raises are pertinent when the issue of consumers’ reactions to architectures of control is raised. From *Persuasive Technology*:

“Interactions created for mobile devices should support an intensive, positive relationship between user and product. Otherwise, the relationship is likely to be terminated, as the device becomes ‘a goner.’ If you viewed a mobile device as part of you, you would expect it to serve you; serving someone else would be a type of betrayal—your device sold you out” [54].

Considering the ethics of the intentions behind persuasive technologies is a central part of captology research; the most favoured examples are those with intended social benefit, and whilst commercial benefit is not decried (especially where it is also helpful to the consumer), subversive uses of persuasive technology for commercial benefit are criticised—for example, Hewlett-Packard’s complex ‘MOPy Fish’ screensaver (which encouraged users to print multiple copies of documents, as

an alternative to photocopying, in return for ‘points’ which would allow the user to ‘buy’ items to enhance the fish’s habitat) [55].

Fogg notes that, “in the future, certain interactive influence tactics are likely to raise ethical concerns, if not public outrage” [56], and, as applied to architectures of control in general, this may well be a significant understatement.

Another commonly cited forcing function for a car ignition is a seat-belt interlock—championed by Lee Iacocca in the 1970’s, and briefly made mandatory on new cars in the United States, but deeply unpopular [32, 35]. “In response to public pressure, Congress took about twenty minutes to outlaw Interlock. They replaced it with an eight-second buzzer that would remind passengers to buckle up” [35].

Whilst there are ways to defeat the interlock on these examples, *e.g.* “many people kept their seat-belts buckled—but without wearing them” [35], depending on how the architectures of control are designed into products, the amount of effort required to overcome them may be too great for most users, even if there are cost or convenience benefits. Apathy, and a fear of ‘meddling’ with devices which may have been an expensive outlay in the first place, may in themselves be significant architectures of control.

Related to interlocks are ‘lock-ins’ (in a different sense to the economic usage mentioned above) and lock-outs. In this sense a lock-in is a forcing function which prevents (or delays) a user from stopping an operation or action which is deemed important. In product terms, an example might involve certain buttons or keys being temporarily disabled, perhaps where accidentally pressing them would be detrimental.

Norman suggested, in 1988, the idea of ‘soft’ off switches for computers, which permit files and settings to be saved before allowing the power to be cut [32], and indeed such soft power switches are now the norm. In terms of control, this can be either useful to the consumer, or an irritation (in cases where a quick power-down is required), but it’s difficult to see it as a strategic architecture of control. Lock-ins with strategic intentions include ‘nag’ screens on software which require the user to wait a certain amount of time before clicking ‘OK’ (*i.e.* exiting the current ‘operation’) in the hope that a promotional message will be read (or that the irritation will become sufficient that the user registers, or pays for, the product [36]). In some cases, this type of lock-in is used to increase (marginally) the likelihood that an EULA will be read, by requiring that the user at least scroll to the bottom before proceeding.

Lock-outs are perhaps more obviously ‘architectures of control’—the aim being to prevent undesirable behaviour or events from occurring. A good example given by Norman is a barrier on a staircase to prevent people, in a panic (*e.g.* in the event of a fire), accidentally running downstairs past the ground floor and into a basement [32].

### **Mistake-proofing**

To a large extent, forcing functions as architectures of control have been inherent in product design and engineering for many decades without necessarily being explicitly recognised as such.

The idea of mistake-proofing, (*poka-yoke* in Shigeo Shingo’s system, as applied at Toyota and other Japanese firms [37]), whilst by no means identical with the idea of architectures of control, is a common theme in design [38], ranging from manufacturing engineering (much machinery cannot be switched on until safety guards are in place) to project management (critical path analysis or Gantt charts to ensure that operations are performed in the correct order) to safety in consumer products (the long earth pin on UK electric plugs enters the socket first and removes the guard which otherwise prevents objects being inserted).

Some would certainly fall into the ‘architectures of control’ category, whether physical (such as cattle-grids), or a combination of physical and psychological (cone-shaped disposable cups, discouraging users from leaving them on tables); particularly in quality management within manufacturing industry, the architectures of control in mistake-proofing (such as designing parts which can deliberately only be assembled one way) are in fact, commercially strategic, since the business’s reputation can depend significantly on maintaining a low error rate in its product assembly. The thinking of ‘design for manufacture and assembly’ promulgators such as Boothroyd and Dewhurst [*e.g.* 39] is evident in many of these often very simple mistake-proofing architectures.

Mistake-proofing and forcing functions in medical environments are also common, both in terms of isolating safety hazards and ensuring procedures are followed. The challenge of retaining these architectures of control once a patient is in charge of his or her own treatment (such as taking the correct dose and combination of pills [*e.g.* 40], or performing particular exercises) should not be underestimated, and is indeed an area of very useful current research [41].

## **New opportunities for architectures of control in products**

The idea of encouraging/incentivising people to exercise (whether for specific medical reasons or on more general health grounds) is a recurring theme, both in gentler ‘persuasive technologies’—see ‘Academic precedents: everyday things and persuasive technology’—and as architectures of control.

Square-Eyes, an electronic children’s shoe insole developed by Gillian Swan at Brunel University, records how many steps the child takes during a day, and ‘translates’ that into a certain number of minutes of ‘TV time,’ with the information transmitted to a base station connected to, and controlling, the television [42]. There is no easy way around it for the child: he or she must exercise in order to obtain the ‘reward,’ and as Tim Ambler points out [43], even ‘cheating’ by, say, jumping up and down on the spot rather than walking or running will still be exercise. All in all, an interesting architecture of control, with possible consequences beyond the child—Brunel Design’s Paul Turnock suggests that “it will raise awareness among the family of their sedentary lifestyle and bring about a change in behaviour for the whole family” [44].

On a more whimsical premise, but retaining the theme of showing how technology is allowing architectures of control to become embedded in design thinking, is Your Turn, a washing machine from Pep Torres of Spanish creative agency De Buena Tinta, which cannot be operated by the same person twice in a row, by using biometric identification. “It’s an invention that has a philosophy behind it and I hope both women and men will think it’s time for the men to do more around the house” [45].

Would this kind of system have been conceivable on a consumer product twenty years ago? Possibly, but perhaps the widespread use of passwords and identification systems, and the apparent ease with which they now pervade new technology, has made it much more realistic to consider incorporating architectures of control into new products—right from the concept stage.

## Summary of examples: emergence of intentions

Reviewing the examples across different sectors, a noticeable tension emerges between architectures of control with primarily **commercial benefit intentions**, and primarily **social benefit intentions**. For example, it is hard to argue that there was any intended social benefit in DVD region coding [46], but there was an intended commercial benefit. On the other hand, breathalyser interlocks for car ignitions would appear to have mainly social benefit intentions, but depending on which lobby is promoting them (*e.g.* the manufacturers of the product), there could well also be intended commercial benefits. However, since this possibility is inherent in any new technology that is introduced, it has not been explicitly recognised in the table that follows.

The classification according to strategic intentions is an important point, since the results are by no means guaranteed. This is partially due to the uncertainty over how easy it is for an ‘average’ consumer to avoid the restrictions which the architecture of control imposes, or how much work is required to do so—the ‘work factor’ as Bill Thompson puts it [47]. It was easy for people to buckle their seatbelts and then sit on top of them to avoid Lee Iacocca’s Interlock, just as it is easy to walk away from uncomfortable seating at a bus stop; however, it takes more technical understanding to defeat the DRM on some music CDs, for example. So long as only a minority of customers circumvent the restrictions, the intentions may broadly succeed, but when the technical work-arounds suddenly become widely available and easy for non-technical users to exploit (*e.g.* with much peer-to-peer software), then the results can be very different. The following table attempts to classify the examples so far discussed, whilst the fold-out diagram inside the front cover also places the examples in the appropriate position in the commercial-social benefit space, along with further examples from subsequent sections such as the case studies.

‘Social benefit’ intentions are contentious in a number of cases, since even when ‘the public good’ is advanced as a reason for implementing the architecture of control (*e.g.* park benches with central armrests to prevent lying down on them), there is inherently a social disbenefit for certain people. As will become apparent later with the ‘optimum lifetime product’ case study, the idea of social benefit as an intention is more complex than it may initially appear.

## Strategic intentions

Example		Commercial benefit ?	Social benefit ?	Notes on 'work factor'
01	High window sills in classrooms	No	Yes	Difficult for pupil to overcome (e.g. by standing up)
02	Urban planning examples	No	Contentious	Various levels of difficulty
03	Traffic calming	No	Yes	Difficult to avoid unless alternative routes are found
04	Skateboarding deterrents	No	Contentious	Skateboarders will simply find somewhere else to use
05	Public seats to discourage sleeping/long occupation	No	Contentious	Users will simply find somewhere else
06	Seats to discourage long occupation in cafés, etc.	Yes	No	Customers can patronise another establishment
07	Insurance company monitoring technology in cars	Yes	Yes	Would require technologically astute tinkering to overcome; alternative insurance companies
08	Fair use copying prevention	Yes	No	Depends on level of DRM, but with technical expertise, will be circumvented
09	User access systems	Yes	Contentious	Depends on level of control; even biometrics can be fooled
10	Trusted computing	Yes	Contentious	Currently unclear how difficult it will be to operate successfully outside the system
11	Flexplay self-erasing DVDs	Yes	No	Numerous technical hacks possible to circumvent this
12	DVD Region coding	Yes	No	Circumvention methods fairly widely known
13	Analogue hole prevention (multiple types)	Yes	No	Alternative products available (for now)
14	Cameras which censor certain images	Yes	Contentious	Alternative products available, even if that means using film
15	Child-proof lids and car door locks	No	Yes	Not difficult for an intelligent child to defeat; the lids can also lock-out those with arthritis
16	Audi A2 bonnet	Yes	No	Alternative products available
17	Replacement parts lock-in	Yes	No	Depending on the product, there are ways round this with varying difficulty
18	Safety forcing functions	No	Yes	Varying levels of difficulty to defeat, but little incentive to do so
19	Seat belt-ignition interlocks	No	Yes	Easy ways around this
20	Breathalyser-ignition interlocks	No	Yes	Some ways around this but require extra technical ability
21	Cattle-grids	No	Yes	There was a sheep which learned to roll across a cattle-grid...
22	Cone-shaped disposable cups	No	Yes	Only a (weak) psychological barrier operates here
23	Square-Eyes insole/TV control	No	Yes	Ingenuous children will find a way round it
24	Your Turn washing machine	No	Yes	Alternative products available

There is an interesting additional facet to the notion of commercial benefit. Whilst the obvious commercial benefit from many architectures of control comes from either preventing copies being made (thus—following an assumption of perfect substitution—increasing sales by one unit for every copy prevented) or forcing consumers to buy replacement parts (thus also increasing sales), there is also the possibility of a strategic commercial benefit through shifting the balance of power in the development of future technology. Andreas Bovens (*q.v.*) quotes (in relation to DRM in the Japanese mobile phone industry—see ‘Reactions’), a *Copyright* article by Ernest Miller which touches on this idea:

“...DRM provides the content industries benefits that are unrelated to or only loosely related to stopping content from getting onto filesharing networks...By insisting on [DRM] the content industries are in a much better position in negotiating how technology will be permitted to develop. If the content industry thinks that a particular new device is too disruptive, they can lock it out of using their DRM’d content legally, something that copyright law would otherwise not allow” [48].

Bovens comments that:

“In other words, broadcasting companies (and other content providers) can use DRM as a tool for protecting their business model by outlawing devices that allow their content to be used in too innovative ways—without DRM, the broadcasters’ attempts to influence the technology companies would have far less effect” [11].

This idea—in effect, innovation lock-out—is applicable beyond simply the commercial aims of content providers. Rival technology manufacturers employ similar methods to prevent their hardware being usable in interaction with rivals’ devices: for example, Sony’s decision to use its own proprietary memory stick format in many of its products rather than the more common SmartMedia or SD cards. This, in turn, prevents any new



developments using the technology outside of the company's control. Where innovation does occur in this realm, using a company's products but outside of its own development teams, reactions range from threats of legal action (e.g. the Sony Aibo robot dog hacks [49]) to the developments being gratefully taken on board by companies eager to incorporate customers' innovations—a strategy developed much further in the work of MIT's Eric von Hippel (see below).

### **Academic precedents: the democracy of innovation**

Eric von Hippel of MIT has charted the phenomenon of user-led innovation, and how this has benefited both companies and users, in *The Sources of Innovation* [57], published in 1988, and, most recently, *Democratizing Innovation\** [58]. As discussed in the 'Reactions' section of this paper, whilst the trend for users to modify and tinker with their products to improve them or create new functions does not yet appear to have abated in an age of increased architectures of control, there is reason for concern—von Hippel notes, with an interesting example, that:

“Current efforts by manufacturers to build technologies into the products they sell that restrict the way these products are used can undercut users' traditional freedom to modify what they purchase... Makers of ink-jet printers... may add technical modifications to their cartridges to prevent them from functioning if users have refilled them. This manufacturer strategy can potentially cut off both refilling by the economically minded and modifications by user-innovators that might involve refilling... [such as refilling] cartridges with special inks not sold by printer manufacturers in order to adapt ink-jet printing to the printing of very high-quality photographs. Others have refilled cartridges with food colourings instead of inks in order to develop techniques for printing images on cakes” [59].

It is not unlikely that future studies by von Hippel or others working in this field will document ingenious user innovation in spite of architectures of control; the challenge may be a sufficient lure in itself for some technical users.

*\*I have retained the US spelling for this title*

## Reactions

An awareness of architectures of control in products, especially digital technology, has been growing significantly over the past few years, as the ‘Academic precedents’ vignettes show. Perhaps unsurprisingly, some of the strongest reactions have propagated in and been disseminated through internet communities, especially those at the intersection of technology and policy thinking.

### The technical community’s reactions to architectures of control

‘Hacker’ culture may be commonly associated only with computers (and generally, by the media, in a negative and incorrect way), but in the correct sense of a culture of technical exploration, experimentation and the innovative testing of rules and boundaries, it is as evident in the young child who uses a stick to retrieve a confiscated football from a high shelf as in Richard Feynman determining how to retrieve secret documents from locked drawers at Los Alamos [63]. The Norwegian teenager working out how to get DVDs to play on his GNU/Linux box [e.g. 64] is not too far removed from the group of engineering students working out how to lift an Austin Seven van onto the roof of Cambridge’s Senate House [65].

There is no malicious intent: whether the attitude is Eric Raymond’s, that “the world is full of fascinating problems waiting to be solved” [66] or even Feynman’s “pleasure of finding things out” [67], much ‘hacking’ is simply the use of ingenuity in an attempt to understand products and systems more fully—indeed, an attempt to *grok*, in Robert Heinlein’s very useful terminology [68]. This fuller understanding can come through—and make possible—finding ways around the embedded architectures of control, with the result of freeing or improving information or functions that are being restricted or are obviously not optimised to the user’s advantage.

Another way of phrasing this might be to say that ‘reverse engineering’ (as demonised by so many EULAs) is not easily separable from ‘forward engineering’—almost all engineering projects depend on understanding of prior art to facilitate a new or improved function. To borrow twice, rather convolutedly, from Isaac Newton: there are many layers of innovators standing on each other’s shoulders, being supported by previous ingenuity and in turn supporting future innovators to see shinier pebbles further along the sea shore.

Specifically, many architectures of control in products (and software) are intended to remove what Edward Felten calls the ‘freedom to tinker’ [69]: the Audi A2 bonnet (*q.v.*) is a high-profile example, but even Apple’s deliberate design of the iPod to

make battery replacement by the user a difficult task [e.g. 70] counts here as part of a trend to move product sovereignty away from the user and into the hands of the ‘experts’.

Whilst individual architectures of control—especially those backed by major companies, such as trusted computing and various DRM methods—have received public support from some ‘technical’ commentators, the most vocal reactions from the technical community are generally very wary of the impact that architectures of control may have on innovation and freedom. For some, such as the Electronic Frontier Foundation, the fight against restrictive or repressive architectures of control is framed within a larger legal and civil rights context—“educat[ing] the press, policymakers and the general public about civil liberties issues related to technology; and act[ing] as a defender of those liberties” [71]. The ‘chilling effects’ [72] on innovation and cultural development caused by challenges to liberties, whether through architectures of control, or regulation, or both, are part of the debate, especially where ‘invisible’ (or perhaps, ‘opaque’) disciplinary architectures can effectively enforce norms as if they were regulation; as Lawrence Lessig says (specifically in relation to the architecture of ‘cyberspace,’ but nevertheless pertinent to disciplinary architectures in general):

“We should worry about this. We should worry about a regime that makes invisible regulation easier; we should worry about a regime that makes it easier to regulate. We should worry about the first because invisibility makes it hard to resist bad regulation; we should worry about the second because we don’t yet... have a sense of the values put at risk by the increasing scope of efficient regulation” [73].

Equally, there are others for whom the effects of architectures of control on the freedom to innovate predominate in the debate. User-driven innovation (ranging from the development of pultrusion machinery highlighted by Eric von Hippel in the 1980s, to the phenomena of ‘innovation communities’ and ‘democratised innovation’ that he has more recently formalised [58]) is certainly challenged by the rise of architectures of control in products and software—for example, Hal Varian’s comment on some mobile phones which detect (and refuse to operate) if a non-recommended brand of battery is used:

“What about cellphone batteries? There are now hand pumps that allow you to produce enough juice to charge your own batteries. Inventors are experimenting with putting such pumps in your shoes so you can charge your cellphone by merely walking around. This would be great for users, but it is hard to experiment with such technologies if you can use only certain power sources in your cellphone” [74].

The success of O’Reilly Media’s MAKE magazine [75]—“technology on your time”—aimed at independent technical enthusiasts and hobbyists from a range of skill levels, with each issue detailing user modifications to existing products (many of them computer-based), new developments in engineering and technology, and simple construction of entirely new projects, indicates that democratized innovation is perhaps a real field of growth, especially if the irritation level of some architectures of control is sufficient to drive people to find ingenious ways around them through tinkering. MAKE has 25,000 subscribers after 4 months, as opposed to O’Reilly’s estimate of 10,000 after a year [76].

Indeed, Richard Stallman’s foundation of the free software movement—perhaps the archetypal user-driven innovation community—was, in a sense, a reaction to the imposition of a contractual architecture of control (the more restrictive Lisp licensing implemented by Symbolics on MIT’s AI Lab [77]).

It is possible, then, that many in the technical community will relish the challenges set by increased use of architectures of control, and much good work may come from this; however, for the non-technical consumer, the challenges may lead to frustration and exclusion, as will be examined in the next section.

(One might argue that in-built restrictive architectures have actually encouraged innovation—would there have been so many groups dedicated to unlocking the iPod’s secrets if the architecture had been entirely open?—but this seems to be analogous to arguing that war is something to encourage because it forces innovation and resourcefulness: is there not a better way to achieve the same desirable results?)

Overall, much of the technical community’s (cautious) reaction to architectures of control can be summed up by Paul Graham’s comments—suitably annotated and with emphasis added:

“Show any hacker a lock and his first thought is how to pick it. But there is a deeper reason that hackers are alarmed by measures like copyrights and patents [or, in this case, architectures of control]. They see increasingly aggressive measures to protect “intellectual property” [and indeed, economic or politically strategic intentions] as a threat to the intellectual freedom they need to do their job. And they are right... *It is by poking about inside current technology that hackers [and engineers, and designers] get ideas for the next generation*” [78].

### **Consumers’ reactions to architectures of control: DRM**

If consumers are aware that their behaviour is being restricted, and the idea is presented in this way, then negative reactions to technology are likely to arise—to the level of an increasing frustration, perhaps even resistentialism [79]. Now that she is a consumer rather than chairman of the RIAA, even Hilary Rosen is apparently dissatisfied with how Apple’s iPod DRM is restricting her behaviour—“Why am I complaining about this? Why isn’t everyone?” [80]

Perhaps because of Apple’s phenomenally successful iPod marketing over the past couple of years, the product (along with iTunes) is rarely out of the news: hence, consumers’ reactions to Apple’s architectures of control (and DRM in music more generally) have been widely circulated. It is not unreasonable to assume that this body of reaction may be taken as indicative of the trends that will become apparent over the next few years as DRM and other architectures of control with little obvious social benefit spread to more consumer products.

*PC Pro* magazine’s widely publicised investigation of the UK’s online music market in April 2005 revealed significant consumer frustrations—some with the fidelity of the (usually lossy) downloaded tracks, but many with the product lock-in enforced by DRM and format-based architectures of control:

““What people don’t understand is that when they buy an iPod or other digital music player, they’re being tied into a system,” believes Deputy Labs Editor, Nick Ross... One *PC Pro* reader spent

£40 downloading music from an online store only to find that although his MP3 player played Windows Media Audio (WMA) files that he created, it wouldn't play the copyright-protected WMA files he'd bought. 'What was I supposed to do,' he said, 'take them back to the shop? It's way too confusing'" [81].

Comments from members of the public in response to BBC News coverage [82] of the *PC Pro* story reveal more of the same concerns, along with a tale of a whole (paid-for) music collection being automatically, irretrievably, locked up due to using Windows' System Restore function.

There is praise for the convenience of being able to download one track at a time as opposed to having to buy whole albums as with a CD, but dissatisfaction with the level of information provided to consumers: how can fairly technical restrictive architectures of control be presented in a way that is easy to understand for the average consumer, whilst not putting him or her off the purchase through negative or complicated language?

This may well be a marketing problem that companies employing restrictive architectures will have to consider very carefully: trusted computing can at least be presented as offering 'security' (however vague or even erroneous that may be), but it may be difficult to maintain the 'convenience' theme with DRM'd music or movies so long as there are less restrictive alternatives available—and especially if those alternatives are familiar and easy to use, such as CDs. One consumer's reply to the BBC story sums this up:

"The whole concept is ridiculous. Would you really buy a CD that you could only play on one brand of CD player? That you couldn't play in the car as well as at home and in your CD Walkman? A CD that has sound quality comparable to an old cassette tape at best? No, no, no!" [82]

Steve Portugal, a customer research consultant whose work often employs ethnography and consumer behaviour studies to advise on product strategies, agrees that, because of consumers' reactions, restrictive architectures of control may not necessarily offer companies the economic benefits intended:

“Products that surprise us with limitations in what we get, what we can do, what is expected, etc. will be met with disappointment, frustration, complaints, and perhaps abandonment. Companies will need to think carefully about setting and managing expectations, although even the best plans can go wrong once a ‘risk’ enters the zeitgeist” [33].

However, he concedes that there is plenty of opportunity for increased use of architectures of control, simply because of consumers’ non-technical indifference or lack of time or motivation to understand the implications of what they are buying:

“It always pays to remember that people are busy, they aren’t thinking about technology, only a very very few want to think about it, want to understand the details and the risks, etc. There’s a minimum activation energy around an issue such as privacy or cost-rip-off that is set higher than we’d like to believe, most of us, and right now, the space under that level is there for the exploiting” [33].

Once an architecture of control becomes very common, there is the possibility that it is no longer noticed by consumers, and indeed is never questioned. This idea is, of course, a mainstay of Orwell’s *1984*, and much subsequent science-fiction, and as applied to certain ideas and taboos, is central to Paul Graham’s classic *What You Can’t Say* [83].

Nevertheless, in certain societies where products have incorporated restrictive architectures of control for a number of years, it is worth examining to what extent the restrictions have become ‘normalised’—Japan is the prime example, since, as Andreas Bovens notes:

“[many new] devices are first launched on the home market and distributed internationally at a later time. Thus, investigating Japan’s current technological landscape gives us an outlook on the content processing devices we might expect to appear in other markets within a short time frame” [11].

Sony's Librié eBook reader, with extremely restrictive DRM (e.g., books stored are automatically locked up after two months, thus requiring re-purchase), has not proved popular on the Japanese market—partially, Bovens suggests, because there are (currently, at least) alternatives available which don't feature the same architectures of control. However, the market for *chaku-uta*, mobile phone 'ringtunes' which are versions of the original tracks, has grown very quickly, even though they too are subject to restrictive DRM:

“heavily DRMed *chaku-uta*... downloads break all records; the same is true for mobile games: they are DRMed but nobody seems to care, even if it means they'll have to buy them again when they switch to another cell phone [2.6 years on average]” [84].

As phones, music/game/video players and PDAs converge, it will be interesting to see whether a generation of children grows up believing it to be perfectly normal to lose all the content acquired each time the device is replaced—at an abstract level, will the mental boundaries of what property is change? (This idea will be mentioned again in the 'Some implications of architectures of control' section).

### **Consumers' reactions to architectures of control: external control**

Some of the most extreme consumer reactions may be expected to occur where the architectures of control in products explicitly remove control from the user and pass it to an outside party.

One method of achieving this may be products which only continue to function if mandated software updates are automatically downloaded, such as the TiVo—this becomes contentious when the software update explicitly changes the product's functions from the feature set with which it was originally purchased, with commercial benefit intentions.

With the TiVo, an automatic update in autumn 2004 “puts restrictions on how long your DVR [digital video recorder] can save certain kinds of shows—so far, just pay-per-view and video-on-demand programs” [85]. However infrequent such function-limiting updates might be, the feature set of the product has been changed, and any attempt to avoid this change (e.g. by unplugging the TiVo from the telephone line to prevent the update occurring) will cause the product to cease functioning entirely, thus removing all the features purchased. Whatever dissatisfaction consumers may have with



this, there are alternatives, such as other personal digital video recorders—although none with quite the TiVo’s combination of attributes—or, for more technically inclined consumers, building a custom “home media convergence box” using software such as the MythTV suite [86].

The case of external control which is arguably most likely to cause a widespread consumer reaction, outside of technical users, is the External Vehicle Speed Control system—with intended social benefits—proposed by Oliver Carsten at the University of Leeds’ Institute for Transport Studies. This is perhaps one of the most clear-cut examples of a disciplinary architecture of control:

“An on-board vehicle speed limiting mechanism may be interfaced to data supplied by roadside infrastructure to provide a method of enacting dynamic local road speed limits to:

- reduce excess speed
- control speeds around an accident site or environmental hazards
- manipulate traffic flows” [87].

Carsten’s own survey, involving both members of the public and representatives from the police, motoring and motorcycling organisations and environmental groups, concedes that:

“[There is] a general resistance to the concept of speed control... it was suggested that a system such as speed control that takes control away from the driver could lead to the loss in [*sic.*] skills in ‘reading the road’” [87].

There are also many possible implications and concerns relevant to this type of system, into which there is insufficient scope to go here, ranging from attribution of accident liability, to the level of driver control (to what extent can he/she disable the system?), to implementing reliable fail-safes in the system, to the costs of installing and operating the hundreds of thousands of roadside ‘beacons’ that Carsten proposes (an alternative being a GPS-based architecture).

Nevertheless, the EVSC system as proposed by the final (July 2000) Carsten report to the Department of the Environment, Transport & Regions suggests “mandatory

usage” in 2019. The report—interestingly—includes a disclaimer to the effect that:

“EVSC has the potential to bring about a very considerable accident reduction, but that potential can only be realised, if in the end there is public support for the introduction of EVSC” [88].

As of 2005, “no policy decision has been made on whether or not to move ahead with the implementation of such a system for the vehicles on Britain’s roads” [89], but whether or not that ‘public support’ is eventually forthcoming, the most vocal reaction so far has been entirely opposed to the system, with the 2001 International Motorcyclists’ Public Policy Conference at Mulhouse declaring its opposition to the proposals and creating a petition including the line, “We note with extreme concern the tendency of governments to impose ever more intrusive and restrictive regulations upon the citizen” [90].

Regardless of the safety benefits of speed control (and the public, if surveyed, would possibly approve of the speed control on buses, coaches and trucks), it is surely the external part which will cause the most consternation if the EVSC plans do proceed further. Architectures of control which fall into this category may be the hardest of all for consumers to accept; it is taking the concept of the ‘nanny state’ to a limit where the nursery is teetering on the brink of rebellion.

## Case study: printer cartridges

Printer cartridges are a consumer product category with a variety of architectures of control exhibiting characteristics discussed in this paper. Aside from the obvious economic lock-in (the razor blade model), there are some specific implementations that are worth detailing further (all are assumed to have commercial benefit and little social benefit; see the fold-out diagram for their positioning):

	Example	Details	Notes on 'work factor'
25	Canon (Japan) printers detect whether or not genuine Canon replacement cartridges are used (the 'handshake'), and refuse to print if a non-Canon cartridge (often cheaper) is detected.	The Japanese Fair Trade Commission is investigating. Canon has previously lost a case over whether external companies recycling (refilling) Canon brand cartridges infringes Canon's intellectual property rights [98].	Refilled cartridges retaining 'genuine Canon cartridge' chip possible; Self-refilling is also possible.
*	Lexmark laser printers perform a handshake with cartridges and will not operate with cartridges identified as non-Lexmark. Static Control Components replicated handshake to enable replacement cartridges to work with Lexmark printers [99].	Lexmark sued SCC under the DMCA; the sale of the SCC handshake chips was banned but the ban was lifted on appeal. "The DMCA was not intended to create aftermarket electronic monopolies...[this] is a major victory for the consuming public and American companies" (Ed Swartz, SCC chief executive) [100].	Alternative laser printers available which do not have a handshake function.
26	Some Hewlett-Packard printers report that printer cartridges need replacement and also shut down the cartridges at a predetermined date regardless of whether they are empty—even if have never been used.	The argument could be made that this is to protect the consumer from a cartridge that no longer functions properly due to ink becoming denatured or the print head blocked, but this is a rather weak benefit for the consumer. A Georgia woman is currently suing Hewlett-Packard over this issue, with the suit seeking class-action status [101]	Providing consumers know to avoid Hewlett-Packard printers with the expiration function, they can choose alternatives.
27	Some manufacturers which produce printers and cartridges under different brands with different pricing levels allegedly permit the cheaper brand's cartridges to function, but make sure the print quality is poor to discourage consumers from further purchases.	"I have a Dell AIO 920... which is a rebadged Lexmark 1150. Local PC store does Lexmark cartridges for the 1150 that fit the Dell—almost. The cartridge is identical apart from the top cover—it's a recessed 'U' shape on the Dell cartridge, but has a raised diagonal plastic tab on the Lexmark—upshot is, you load it in, close the lid, and all your printing is badly misaligned (colour against black). No way of adjusting it to fit with the supplied software as it is so far out of alignment" [102].	"Solution? Snap off the diagonal tab—works a treat!" [102]  However, if this had been a software issue rather than a simple physical one, there may not be such an easy work-around.

*\*This is an example of a company producing a work-around for an architecture of control rather than an architecture of control itself, so has not been included on the numbered list or the fold-out diagram*

## Some implications of architectures of control

How will increased use of architectures of control in the design of products change the way we live? Depending on how pervasive they are, and how feasible the alternatives are, there is the possible emergence of two tiers of technology consumers—those who embrace products with architectures of control, with the (real or imagined) benefits that may offer them (for example, exclusive content, the ‘security’ of trusted computing, or simply network effects)—and those ‘excluded consumers’ who either stick to using older technology free of control, or (depending on legality) buy new, probably premium-priced, ‘professional’ equipment which is similarly free of control. It may become a vanity for the technical connoisseur—similarly to the way that valve amplifiers or the ash frame of the Morgan sports-car are today revered.

But where would this leave consumers who actually depend on the freedoms that are taken away by many architectures of control, through disability, for financial reasons or simply for reasons of social good? Will a ‘technology underclass’ become apparent? Will screen-reader software for the partially sighted work in a world of tightly restricted eBooks? Precedents set by existing DRM would suggest significant problems in this area—to the extent that the UK’s Royal National Institute for the Blind is currently compiling a report on “how widely used DRM systems block access by blind or partially sighted people” [91]. Will sharing books be possible with Sony Librié eBooks that expire after a couple of months? How will the PCs currently being donated for educational use to developing countries worldwide be affected when everyone else is using ‘trusted computing’? How will a buyer of a used Audi A2 fifteen years from now cope with the bonnet constraint? And, as raised earlier, how will DRM and ‘unpublishing’ affect archiving and accountability?

One conclusion which it is possible to draw from many of the architectures of control examined so far is that the relationship between the consumer and his or her ‘products’ (and the content used on them) is gradually changing. Whereas buying an LP gave the consumer a permanent, physical copy of that music, which could be played on a variety of devices, and resold or lent or destroyed or recorded onto tape at will (whether or not each of those activities was legal), buying music or other content now is effectively buying a very limited licence to use it which is enforced by the architectures of control in both the content and the device on which it is used.

Extending this to some of the other architectures of control, it becomes a possibility that consumers are no longer buying products, but effectively *licensing the*

*functions those products provide* [92]. This idea will be developed further in ‘Case study: ‘optimum lifetime products’’ but it is worth noting here Bill Thompson’s tentative suggestion [47] that perhaps this is part of a wider trend of society moving away (or being moved away) from the individual sovereignty property régime of the last few hundred years—increasingly, control of the technology will be in the hands of the ‘experts.’

What do designers themselves think the implications of architectures of control might be? Do they see them as a useful set of additional tools for building into future products?

Chris Weightman, an industrial designer at London consultancy Tangerine, believes that outside of the companies that have gone strategically (and perhaps philosophically) down the DRM and restriction route, designers will generally tend to focus on making the product experience more attractive to the user, with easier interactions a goal of many briefs. This tends to work against many architectures of control: indeed, there may well be a commercial advantage to being ‘second’ in the market (a ‘me-too’ product) but offering a simpler, more open product:

“The only distinctive selling point of some companies’ products—particularly in the portable music player market—is that they allow the user to get round the restrictive architecture of the market leaders. If design can build on that distinctiveness by making the product appealing in other ways as well, then second place could well become first place” [93].

All this assumes that there is still the legal freedom to pursue strategies outside of using architectures of control, which in certain sectors, may not be the case. If External Vehicle Speed Control (*q.v.*) becomes mandatory on new cars, for example, there is no legal market position for a company producing vehicles without EVSC (although one might suggest a limited market for a company which reconditions and refurbishes pre-EVSC cars to a very high standard—giving the ‘new car’ experience, complete with warranties, but on vehicles which are legally deemed to be ‘old’).

A parallel development may be the use of architectures of control to empower the consumer in some way—an example being the ‘knee defender’ now available for airline

passengers to set the angle which the passenger in front can recline his or her seat [94]. Here, the consumer is applying an architecture of control, perhaps in an arbitrary way, but it sets the scene for a plethora of innovation, possibly from small companies, to impose control on the surrounding environment or overcome architectures of control that have been built into that environment by others. It may spiral into a cycle of competing architectures and methods of defeating them—speed cameras, then the slave-flash for car number plates which would defeat the speed cameras [95], and so on.

Indeed, the opportunity may be there for innovative small companies to exploit the concern or paranoia which has led to the imposition of the architectures of control in the first place. It may be an entrepreneur whose breathalyser interlock persuades legislators to regulate on this issue, for instance.

Or, by extension, a small company which offers large corporate customers a way (real or perceived) to reinforce the superiority of their product (*e.g.* music, films, consumer electronics and even cosmetics) over illegal copies, could be extremely successful. Hamish Thain, a designer at the innovative packaging firm Burgopak [96, 97], makes the point that by offering third parties a distinctive, patented packaging system, those third parties can enhance and protect the value of their own products when compared to unauthorised copies or 'knock-offs.' Targeting clients (including Microsoft, Sony and numerous record companies) who are at the forefront of the intellectual property protection debate leverages—and satisfies—that corporate concern, whilst at the same time enabling a smaller innovator to succeed. Whilst this may not be Burgopak's explicit strategy—and is, of course, not an architecture of control in itself—it demonstrates the fluidity of a situation where the motivations that lead to architectures of control can be exploited.

## Case study: 'optimum lifetime products'

Despite consumer frustration when they break, many products are designed and built to last far longer than might be considered 'environmentally optimum.' Simply put, if technology in a certain field is advancing at a rate such that newer products use less energy (in manufacture and use) than old ones (which may also be using increasingly more energy due to wear and tear), there will come a point where comparatively, it is more environmentally beneficial to replace older products (and recycle them to recover as much embodied energy as possible) with new ones [103].

Of course, encouraging consumers to replace their products with new ones is also the goal of many companies and their design and marketing teams, for purely commercial reasons. But what if these interests were to be dovetailed—the social benefit intentions of an environmentally optimum lifetime for a product, and the commercial benefit intentions of managed replacement times?

An optimum lifetime product could 'expire' at the point when its optimum lifetime is reached (based on actual usage rather than averages for the sector, so as not to antagonise light users)—thus minimising the environmental damage caused. The architecture of control would prevent further usage.

Would consumers put up with this? David Harrison, who has worked extensively on technology for sustainable product design, including active disassembly and conductive lithography, comments that, "having a machine that decided when its lifetime was up, though was capable of working well, could be extremely frustrating" [104]. Nevertheless, when the idea is considered in the light of the end-of-life take-back legislation for cars and other products (e.g. the Waste Electrical and Electronic Equipment directive [105]), a more

coherent scheme emerges: products which have a pre-determined lifetime (based on usage) and once that lifetime is up, they are returned to the manufacturer (perhaps the products even signal to the manufacturer that they are reaching expiry). The product could then be replaced, or a different model chosen, maybe depending on a licence agreement the purchaser has with the manufacturer or supplier. In effect, the consumer is simply renting the functions the product provides.

A system such as this would have to offer the consumer sufficient obvious benefits to be appealing enough to sign up to a rental-style agreement in the first instance. Whilst products which are always in an optimum state of efficiency would save some energy costs, this is unlikely to provide sufficient motivation. However, if the product's original warranty were to be extended to cover the entire lifetime of the product until it expired, then this might be incentive enough—along with the promise of a shiny new replacement every few years. The consumer would be renting the functions required, with no worries about servicing or maintenance; the manufacturer or retailer would have guaranteed income and a guaranteed outlet for its future products, plus full control of recovering (and recycling, cannibalising—or perhaps reconditioning?) the expired products (which presumably would have restrictions applied on issues such as customer modification, disassembly or customisation).

As has been touched upon earlier, would a much more common use of this kind of architecture of control, in conjunction with the rental model, lead to a noticeable change in consumers' attitudes to property? Would no longer owning much of the technology used in everyday life (cars, computers, white goods,



and so on) have a psychological impact on consumers' attitudes to those products? There are so many possibilities, including users deliberately accelerating the expiry of their products to hasten the arrival of a brand-new replacement, that a much deeper investigation of the idea is worthy of consideration.

Equally deserving of consideration, of course, is to what extent the social benefit of better environmental performance would be negated by the welfare issue of locking poorer consumers into expensive product replacement cycles which do not individually benefit them. A family whose washing machine automatically expires even though it still worked perfectly, and who are unable to afford to keep paying the licence, may be better served by a functioning, inefficient machine than by the larger environmental benefit of a non-functioning machine.

There are some much less complex architectures of control in products which could also achieve social benefits in terms of lessening environmental damage. Office lighting could automatically switch off if no-one was in the room, or if the level of sunlight were detected to be above a certain threshold. A car throttle could prevent excessive or unnecessary revving. Alternatives which lessen the 'control' aspect could include devices which simply warn users about how they are being operated, for example a refrigerator with an alarm which sounds if the door is not closed properly, or built-in electricity meters on household plugs. Even rubbish bins could be made smaller to make consumers more aware of how much they are throwing away.

### Strategic intentions

	Example	Commercial benefit?	Social benefit?	Notes on 'work factor'
28	Expiry of products at optimum lifetime (as part of 'rental' scheme)	Yes	Yes	Alternatives would be available outside of the rental scheme, and illicit hacks would undoubtedly arise to delay expiry.
29	Lighting automatically switching off	No	Yes	An over-ride may be built in.
30	Car throttle preventing excessive revving	No	Yes	Unless monitored, would probably be fairly easy to circumvent.



## Conclusion

This has been a rapid look at product design in some diverse areas, with the architectures of control perhaps, initially, not obviously sharing many characteristics. However, a picture does emerge from the glimpses of fields ranging from motoring to the music industry, exercise promotion to the environment.

Control of the public's behaviour—whilst nothing new—now has the potential to be much more widespread, through the use of design and technology to change the relationship between consumers and products. Whether for purely commercial benefit or 'the greater good,' whether by companies or by governments, architectures of control have the power to affect our lives. The phenomenon deserves recognition.

## References

1. WINNER, L. 'Do artifacts have politics?' in *The Whale and The Reactor: A Search for Limits in an Age of High Technology*, University of Chicago Press, Chicago, 1986
2. 'Baron Haussmann' entry on Wikipedia, 10. iv. 2005, [http://en.wikipedia.org/wiki/Baron\\_Haussmann](http://en.wikipedia.org/wiki/Baron_Haussmann)
3. JACOBS, J. *The Death and Life of Great American Cities*, Pelican Books, Harmondsworth, 1965, pp. 99-100
4. EWING, R. *Traffic Calming: State of the Practice*, Institute of Transportation Engineers, Washington D.C., 1999
5. HOWELL, O. 'The Poetics of Security: Skateboarding, Urban Design, and the New Public Space,' *Urban Action* 2001/San Francisco State University Urban Studies Program, 2001, <http://www.urbanstructure.com/urbanaction/PS.html>
6. 'Recycled Plastic Georgetown Bench,' *Belson Outdoors, Inc.*, acc. May 2005, <http://www.belson.com/gbrec.htm>
7. BENTHAM, J. 'Panopticon; or The Inspection-House, &c.' in *The Panopticon Writings* (ed. Miran Bozovic), Verso, London, 1995
8. FOUCAULT, M. *Discipline and Punish: Birth of the Prison* (tr. Alan Sheridan), Peregrine Books, Harmondsworth, 1979
9. 'What is Traksure?' AXA Insurance Limited (Ireland), acc. May 2005, <http://www.axa.ie/car/traksure.html>
10. 'Pay As You Drive™ insurance,' Norwich Union, acc. May 2005, <http://www.norwichunion.com/pay-as-you-drive>
11. BOVENS, A. 'Closed Architectures for Content Distribution,' *Japan Media Review*, 12. ii. 2005, <http://www.japanmediareview.com/japan/stories/050210bovens>
12. von LOHMANN, 'Fair Use and Digital Rights Management,' *Electronic Frontier Foundation*, 16. iv. 2002, [http://www.eff.org/IP/DRM/cfp\\_fair\\_use\\_and\\_drm.pdf](http://www.eff.org/IP/DRM/cfp_fair_use_and_drm.pdf)
13. MAGID, L. 'It Pays To Read License Agreements,' *PC Pitstop*, acc. May 2005, <http://www.pcpitstop.com/spycheck/eula.asp>
14. STALLMAN, R.M. 'The Right to Read,' *Communications of the ACM*, Vol. 40, No. 2, February 1997, <http://www.gnu.org/philosophy/right-to-read.html>
15. ANDERSON, R. "'Trusted Computing' Frequently Asked Questions,' Version 1.1, August 2003, <http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>
16. TOURETZKY, D. 'Gallery of Adobe Remedies,' 8. iv. 2005, <http://www-2.cs.cmu.edu/~dst/Adobe/Gallery>
17. 'End the hassle of renting movies with

- the Flexplay DVD,' Flexplay, acc. May 2005, <http://www.flexplay.com>
18. 'Digital Rights Management' entry on Wikipedia, 30. iv. 2005, [http://en.wikipedia.org/wiki/Digital\\_Rights\\_Management](http://en.wikipedia.org/wiki/Digital_Rights_Management)
19. MEDLAR, A. 'Adobe forbids reading aloud,' 13. xii. 2000, <http://www.pigdogs.org/art/adobe.html>
20. SCHNEIDER, N. 'The Sound of iPod,' 11. i. 2005, <http://ipodlinux.org/stories/piezo>
21. 'Endangered Gizmos,' Electronic Frontier Foundation, acc. May 2005, <http://www.eff.org/endorsed/list.php>
22. DOCTOROW, C. 'Understanding the Broadcast Flag,' for G4 TV 'Screen Savers,' 15. viii. 2002, [http://www.g4tv.com/screensavers/features/39462/Understanding\\_the\\_Broadcast\\_Flag.html](http://www.g4tv.com/screensavers/features/39462/Understanding_the_Broadcast_Flag.html)
23. DOCTOROW, C. 'Hollywood wants to plug the 'Analog Hole' on 'Consensus at Lawyerpoint,' 23. v. 2002, <http://bpdg.blogs.eff.org/archives/000113.html>
24. GREENE, T. 'Court blasts FCC on broadcast flag,' The Register, 7. v. 2005, [http://www.theregister.co.uk/2005/05/07/broadcast\\_flag\\_shot\\_down](http://www.theregister.co.uk/2005/05/07/broadcast_flag_shot_down)
25. 'Digital Millennium Copyright Act' entry on Wikipedia, 22. iv. 2005, [http://en.wikipedia.org/wiki/Digital\\_Millennium\\_Copyright\\_Act](http://en.wikipedia.org/wiki/Digital_Millennium_Copyright_Act)
26. LESSIG, L. *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*, Penguin Books, New York, 2004, pp. 93-97
27. *ibid*, pp. 96-7
28. *ibid*, pp. 99-100
29. LESSIG, L. *Code, and Other Laws of Cyberspace*, Basic Books, New York, 1999
30. FOGG, B.J. *Persuasive Technology: Using Computers to Change What We Think and Do*, Morgan Kaufmann, San Francisco, 2003
31. 'Fantastic car,' a review of Audi A2 1.4 TDI by user 'Hils303' on Ciao!, 24. i. 2004, [http://www.ciao.co.uk/Audi\\_A2\\_1\\_4\\_TDI\\_\\_Review\\_5381671](http://www.ciao.co.uk/Audi_A2_1_4_TDI__Review_5381671)
32. NORMAN, D. *The Design of Everyday Things*, Basic Books, New York, 2002, pp. 132-140
33. Correspondence between Steve Portigal and the author, April/May 2005
34. BERRIDGE, D. 'Safety First: The SSV/SRV cars,' on the Unofficial Austin-Rover Web Resource, 17. viii.2004, <http://www.austin-rover.co.uk/researchsrvf.htm>
35. IACOCCA, L. *Iacocca, An Autobiography*, Bantam Books, London, 1986, pp. 309-316
36. FOGG, B.J., *supra*, pp. 106-107
37. SHINGO, S. *Study of the Toyota Production System: From an Industrial Engineering Viewpoint* (tr. Andrew P.

- Dillon), Productivity Press, New York, 1989
38. GROUT, J. 'John Grout's Poka-Yoke Page,' acc. May 2005, [http://csob.berry.edu/faculty/jgrout/poka\\_yoke.shtml](http://csob.berry.edu/faculty/jgrout/poka_yoke.shtml)
39. BOOTHROYD, G., DEWHURST, P. and KNIGHT, W.A. *Product Design for Manufacture and Assembly*, Marcel Dekker, New York, 2001
40. BECH, K.S. 'PillAid' in *Good Thinking : Brunel Design 04 Directory* (eds. D. Lockton, C. Weightman, P. Turnock and J.E. Hanson), Brunel University, Runnymede, 2004
41. WARD, J. et al, *Design for Patient Safety*, Department of Health, London, 2003, <http://www-edc.eng.cam.ac.uk/medical/downloads/report.pdf>
42. SWAN, G. 'Square-Eyes' in *Brunel Design 2005* (eds. P. Turnock, A. Bartlett, et al), Brunel University, Uxbridge, 2005
43. AMBLER, T. 'The ultimate incentive to get kids exercising?' on *Principles of Timology*, 18. v. 2005, <http://ambler.ca/weblog/archives/000033.html>
44. 'Shoe kick-starts active lifestyle,' *BBC News*, 18. v. 2005, <http://news.bbc.co.uk/1/hi/technology/4555989.stm>
45. PHILLIPS, V. 'Washing machine fingers lazy male,' *BBC News*, 1. v. 2005, <http://news.bbc.co.uk/1/hi/technology/4504393.stm>
46. SILVA, R. 'Region Codes-DVD's Dirty Secret,' *About.com Home Theater section*, 2. viii. 2004, [http://hometheater.about.com/cs/dvdlaser\\_disc/a/aaregioncodesa.htm](http://hometheater.about.com/cs/dvdlaser_disc/a/aaregioncodesa.htm)
47. Discussion between Bill Thompson and the author, May 2005
48. MILLER, E. 'Why Use DRM If It Doesn't Work?' on *Copyfight*, 7. v. 2004, <http://www.corante.com/copyfight/archives/003559.html>
49. LESSIG, L. *Free Culture*, supra, pp. 97-8
50. LESSIG, L. *Code, and Other Laws of Cyberspace*, supra, pp. 85-99
51. LESSIG, L. *The Future of Ideas: The Fate of the Commons in a Connected World*, Random House, New York, 2001
52. *Stanford Persuasive Technology Laboratory*, <http://captology.stanford.edu>
53. FOGG, B.J., supra, pp. 205-7
54. *ibid*, p. 194
55. *ibid*, pp. 228-9
56. *ibid*, p. 250
57. von HIPPEL, E. *The Sources of Innovation*, Oxford University Press, New York, 1988
58. von HIPPEL, E. *Democratizing Innovation*, MIT Press, Cambridge, Mass., 2005
59. *ibid*, p. 99
60. ODLYZKO, A. 'The Evolution of Price

- Discrimination in Transportation and its Implications for the Internet,' Review of Network Economics, September 2004, [http://www.rnejournal.com/articles/odlyzko\\_RNE\\_sept\\_2004.pdf](http://www.rnejournal.com/articles/odlyzko_RNE_sept_2004.pdf)
61. McKNIGHT, L., LEHR, W.H. and HOWISON, J. Coordinating User and Device Behaviour in Wireless Grids, <http://wirelessgrids.net/docs/BehaviourTechPaperSingle.pdf>
62. GILLET, S.E., LEHR, W.H., WROCLAWSKI, J.T. and CLARK, D.D., 'Do Appliances Threaten Internet Innovation?,' IEEE Communications, October 2001, <http://ieeexplore.ieee.org/iel5/35/20680/00956112.pdf?arnumber=956112>
63. FEYNMAN, R.P. 'Los Alamos From Below,' in *The Pleasure of Finding Things Out* (ed. Jeffrey Robbins), Perseus Publishing, Cambridge, Mass., 1999 (also <http://clsdemo.caltech.edu/14/01/FeynmanLosAlamos.pdf> )
64. LEYDEN, J. 'DVD Jon is free-official,' *The Register*, 7. i. 2003, [http://www.theregister.co.uk/2003/01/07/dvd\\_jon\\_is\\_free\\_official](http://www.theregister.co.uk/2003/01/07/dvd_jon_is_free_official)
65. BALCHIN, N. and DAVY, P. 'A van that went up in the world,' *Gonville & Caius College*, Cambridge, 1996, <http://www.cai.cam.ac.uk/college/past/legend>
66. RAYMOND, E.S. 'How to become a hacker,' *The Cathedral and the Bazaar*, O'Reilly Media, Sebastopol, Cal., 1999 (also at <http://www.catb.org/~esr/faqs/hacker-howto.html> )
67. FEYNMAN, R.P. 'The Pleasure of Finding Things Out,' in *The Pleasure of Finding Things Out*, supra.
68. HEINLEIN, R. *Stranger in a Strange Land*, Putnam Publishing, New York, 1961
69. FELTEN, E.W., *Freedom to Tinker* blog, <http://www.freedom-to-tinker.com>
70. NEISTAT, C.O. and NEISTAT, V., 'iPod's Dirty Secret' (movie), 2003, <http://ipodsdirtysecret.com>
71. 'General information about the Electronic Frontier Foundation,' *Electronic Frontier Foundation*, acc. May 2005, <http://www.eff.org/about>
72. *Chilling Effects Clearinghouse*, <http://www.chillingeffects.org>
73. LESSIG, L. *Code, and Other Laws of Cyberspace*, supra, p. 99
74. VARIAN, H.R. 'New chips can keep a tight rein on consumers, even after they buy a product,' *New York Times*, 4. vii. 2002, <http://www.sims.berkeley.edu/~hal/people/hal/NYTimes/2002-07-04.html>
75. DOUGHERTY, D. (ed.) *Make: Technology on Your Time*, Vol. 01, O'Reilly Media, Sebastopol, Cal., February 2005
76. ROTH, D. 'The Amazing Rise of the Do-It-Yourself Economy,' *Fortune*, May 2005,

- <http://www.fortune.com/fortune/technology/articles/0,15114,1061773-1,00.html>
77. STALLMAN, R.M. 'My Lisp Experiences and the Development of GNU Emacs,' International Lisp Conference, 28. x. 2002, <http://www.gnu.org/gnu/rms-lisp.html>
78. GRAHAM, P. 'Good Bad Attitude' in Hackers & Painters, O'Reilly Media, Sebastopol, Cal., 2004
79. 'Resistentialism' entry on Wikipedia, 11. ii. 2005, <http://en.wikipedia.org/wiki/Resistentialism>
80. ROSEN, H. 'Steve Jobs, Let My Music Go,' Huffington Post blog, 9. v. 2005, <http://www.huffingtonpost.com/theblog/archive/2005/05/steve-jobs-let-.html>
81. 'PC Pro online music exposé: UK public pays too much for too little,' PC Pro, 22. iv. 2005, <http://www.pcpro.co.uk/news/72076/pc-pro-online-music-expos-uk-public-pays-too-much-for-too-little.html>
82. 'Online music lovers 'frustrated',' BBC News, 25. iv. 2005, <http://newswww.bbc.net.uk/1/hi/technology/4474143.stm>
83. GRAHAM, P. 'What You Can't Say' in Hackers & Painters, supra.
84. Correspondence between Andreas Bovens and the author, April 2005
85. GRAVES, L. 'Has TiVo Forsaken Us?,' Wired, November 2004, <http://www.wired.com/wired/archive/12.11/view.html?pg=3>
86. 'What is MythTV?' on MythTV website, 17. v. 2005, <http://www.mythtv.org/docs/mythtv-HOWTO-1.html>
87. CARSTEN, O. and FOWKES, M. External Vehicle Speed Control, Phase I Results, Executive Summary, Institute for Transport Studies, University of Leeds, July 1998, [http://www.dft.gov.uk/stellent/groups/dft\\_roads/documents/page/dft\\_roads\\_506878.pdf](http://www.dft.gov.uk/stellent/groups/dft_roads/documents/page/dft_roads_506878.pdf)
88. CARSTEN, O. and TATE, F. External Vehicle Speed Control, Final Report: Integration, Institute for Transport Studies, University of Leeds, July 2000, [http://www.transport.gov.uk/stellent/groups/dft\\_roads/documents/page/dft\\_roads\\_506877.pdf](http://www.transport.gov.uk/stellent/groups/dft_roads/documents/page/dft_roads_506877.pdf)
89. 'External vehicle speed control project-introduction,' Department for Transport website, acc. May 2005, [http://www.dft.gov.uk/stellent/groups/dft\\_roads/documents/page/dft\\_roads\\_506876.hcsp](http://www.dft.gov.uk/stellent/groups/dft_roads/documents/page/dft_roads_506876.hcsp)
90. LIVERSIDGE, N.F. 'The Mulhouse Declaration,' Motorcycle Action Group, 2001, [http://www.network.mag-uk.org/EVSC/EVSC\\_Mulhouse.html](http://www.network.mag-uk.org/EVSC/EVSC_Mulhouse.html)
91. 'Get involved in RNIB campaigns,' Royal National Institute for the Blind, 4. iii. 2005,

- [http://www.rnib.org.uk/xpedio/groups/public/documents/PublicWebsite/public\\_rnib003590.hcsp](http://www.rnib.org.uk/xpedio/groups/public/documents/PublicWebsite/public_rnib003590.hcsp)
92. Thank you to Peter Moar for this observation.
93. Discussion between Chris Weightman and the author, May 2005
94. Knee Defender website, <http://www.kneedefender.com>
95. 'Backflash' in 'Laser & Radar Review,' Evo, January 1999 (also at <http://www.automotive.co.uk/test5.shtml> )
96. Burgopak website, <http://www.burgopak.com>
97. Discussion between Hamish Thain and the author, May 2005
98. SMITH, A. 'Canon loses printer recycling case,' The Register, 9. xii. 2004, [http://www.channelregister.co.uk/2004/12/09/canon\\_loses\\_printer\\_case](http://www.channelregister.co.uk/2004/12/09/canon_loses_printer_case)
99. 'Lexmark v. Static Control Case Archive,' Electronic Frontier Foundation, acc. May 2005, [http://www.eff.org/legal/cases/Lexmark\\_v\\_Static\\_Control](http://www.eff.org/legal/cases/Lexmark_v_Static_Control)
100. LEYDEN, J. 'Lexmark suffers setback in DMCA case,' The Register, 28. x. 2004, <http://www.theregister.co.uk/2004/10/28/lexmarkvsscc>
101. 'US woman sues over ink cartridges,' BBC News, 24. ii. 2005, <http://news.bbc.co.uk/1/hi/technology/4293427.stm>
102. SHERRIFF, L. 'Things to do online when you're dead,' The Register, 8. ii. 2005, quoting correspondent 'Peter,' [http://www.theregister.co.uk/2005/02/08/letters\\_0802](http://www.theregister.co.uk/2005/02/08/letters_0802)
103. CHALKLEY, A., HARRISON, D. and BILLET, E. A Review of Product Lifetime Optimization as an Environmental Tool, International Conference on Engineering Design ICED01, 2001
104. Correspondence between David Harrison and the author, April 2005
105. 'Directive 2002/96/EC of the European Parliament and of the Council of 27 January 2003 on waste electrical and electronic equipment (WEEE),' Official Journal of the European Union, 13. ii. 2003, [http://europa.eu.int/lex/pri/en/oj/dat/2003/l\\_037/l\\_03720030213en00240038.pdf](http://europa.eu.int/lex/pri/en/oj/dat/2003/l_037/l_03720030213en00240038.pdf)